AFRL-SR-BL-TR-98-

0053

REPORT DOCUMENTATION PAGE

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
		Final 30 Sep 95 to 29 Nov 1997

4. TITLE AND SUBTITLE
PHOTONIC IMAGING NETWORKS

5. FUNDING NUMBERS
61103D
3484/FS

6. AUTHOR(S)
DR FAINMAN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The Regents of the University of California
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0934

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/NE
110 Duncan Ave Room B115
Bolling AFB DC 20332-8050

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
F49620-95-1-0538

11. SUPPLEMENTARY NOTES

19980116 036

12a. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVAL FOR PUBLIC RELEASED: DISTRIBUTION UNLIMITED

12b. DISTRIBUTION CODE

We have selected as a prototype application diagnotic medical imaging and visualization. We have developed several radiological visualization station we have developed and evaluated metholds for the lossless compression of images and image-formate data over a lossy packet network. We have studied noise mechanisms in transparent photonic networks. We have demonstrated parallel-to-serial and serial-to-parallel conversion using spectral domain four-wave mixing with 150 fsec laser pulses reaching serial data rates of over 1 Tbit/sec. we have constructed and demonstrated a nonlinear optical processor based on three-wave mixing in nonlinear LBO crystals. We have employed the parallel-to-serial and serial-to-parallel processors for experimental demonstration of transmission of image information through an optical fiber channel. We have analyzed the secrecy capacity of a quantum cryptographic protocol for secret key generation and found that it primarily depends on estimates of information in eavesdropper's possession, and the expected fraction of inconclusive outcomes. We investigated experimentally a novel frequency division long distance interferometer for implementing quantum cryptographic protocol and found that signals are not affected by transmission over optical fiber, we have developed for the first time the rigorous definitions and the mathematical formalism for information leakage through possible eavesdropping on the quantum channel. We quantify effective defense frontiers against eavesdroppers attacks.

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNBCLASSIFIED	UNCLASSIFIED	UL

Final Technical Report

for

Photonic Imaging Networks

Sponsored by

Air Force Office of Scientific Research

Ballistic Missile Defense Organization

Under Grant F-49620-95-1-0538

for Period 09/30/95 through 11/30/97

Grantee

The Regents Of the University of California, San Diego

University of California , San Diego

La Jolla CA 92093

Principal Investigators:	Y. Fainman	Albert Kellner
	(619) 534-8909	(619) 534-7919
Program Manager:	Dr. Alan Craig	Dr. L. Lome
	(202) 767-4931	

2. Objectives/Statement of work

A. Study scalable network architectures and protocols for third generation photonic imaging networks with special emphasis on terabit networks using ultrashort laser pulses. The study is focused on applications to medical and biomedical imaging and visualization (in collaboration with Brown University).

B. Investigate nonlinear spectral domain processing techniques and interfaces for multiplexing, demultiplexing, encoding, and decoding, to generate data at rates exceeding 1 Tb/sec (in collaboration with Purdue University).

C. Study security and privacy for third-generation photonic networks by investigating methods of quantum and classical cryptography.

D. Investigate wireless-to-photonic networks interfaces for transmission of medical and biomedical images and image format data (in collaboration with UCSD's FRI project on Wireless Communications).

3. Status of effort

A. We have selected as a prototype application diagnostic medical imaging and visualization. We are identifying and quantifying the required quality-of-service. In collaboration with Brown University, we have identified candidate image fusion applications to be implemented over the imaging network. In collaboration with the Department of Radiology at UCSD, we have developed several radiological visualization stations and are evaluating them in clinical environments. We have developed and evaluated methods for the lossless compression of images and image-format data over a lossy packet network. We have developed various methods of constructing transparent optical switching fabrics, including the transparent optical multistage interconnection network and the cascaded optical delay multiplexer. We have studied noise mechanisms in transparent photonic networks (e.g. incoherent phase noise and noise due to multiwave mixing) and have quantified their behavior.

B. We have demonstrated parallel-to-serial and serial-to-parallel conversion using spectral domain four-wave mixing with 150 fsec laser pulses reaching serial data rates of over 1 Tbit/sec. Most recently we have constructed and demonstrated a nonlinear optical processor based on three-wave mixing in nonlinear LBO crystals. The processor operates with femtosecond response time and, unlike commonly used autocorrelators, allows time-to-space conversion of both amplitude and phase information carried by ultrashort pulses. Spectral domain processors have been rigorously analyzed encountering for higher order dispersion. The analytic results have been confirmed by experimental measurements. Finally, we have employed the developed parallel-to serial and serial-to-parallel processors for experimental demonstration of transmission of image information through an optical fiber channel.

C. We have analyzed the secrecy capacity of a quantum cryptographic protocol for secret key generation and found that it primarily depends on estimates of information in eavesdropper's possession, the error correction algorithm employed, as well as line attenuation, detector quality, and the expected fraction of inconclusive outcomes. We investigated experimentally a novel frequency division long distance interferometer for implementing quantum cryptographic protocol and found that the signals are not affected by transmission over optical fiber, thus reducing the channel error rate. We have developed for the first time the rigorous definitions and the mathematical formalism for information leakage through possible eavesdropping on the quantum channel. We quantify effective defense frontiers against eavesdroppers attacks. We have investigated the relationship between the induced error rate and the maximum amount of information the eavesdropper can extract, both in the two-state B92 and the four-state BB84

quantum cryptographic protocols. In each case, a closed-form functional dependence between the error rate and the information yield was found, and confirmed by numerical simulation. The relationship between the induced error rate and the eavesdropper's information on error-free bits can serve as input for the construction of the defense frontier, which has been suggested in our earlier work as a formalism for securing a quantum cryptographic transmission in a noisy environment.

4. Accomplishments/New Findings

In the following we briefly summarize the UCSD's team accomplishments in the main focus areas being investigated under the Focused Research Initiative project: (a) Architectures, Protocols and Applications, (b) Nonlinear Spectral Domain Processing for Multiplexing/Demultiplexing, and (c) Network Security and Privacy .

A. Architectures, Protocols and Applications

In this area, our research is primarily focused on studies of quality of service and image encoding, however the FRI project is also leveraged from our on-going research on transparent optical networks and their various noise characteristics. Furthermore, we designed a demonstration platform for evaluating network algorithms, determining quality-of-service for application in medical imaging (e.g., diagnostic radiology), and evaluating the performance of photonic network devices and subsystems being investigated at UCSD and Purdue.

Delivery of Guaranteed Quality of Service

The concepts of arrival and service curves, developed originally for deterministic quality-of-service guarantees, were extended to include probabilistic quality-of-service guarantees. A mathematically rigorous analysis of window flow control protocols was developed. This provides tight lower bounds on window sizes in order to achieve maximal guaranteed throughput. The so-called "network calculus" was refined, and a novel network scheduling algorithm was analyzed. The proposed protocol supports hard delay guarantees for diverse traffic types without the need for packet switches to write deadlines into each packet, instead relying on devices at periphery of network to write deadlines. This also allows for efficient statistical sharing between best-effort and guaranteed traffic.

Determination of quality-of-service requirements for imaging and visualization environments

Quality-of-service (QOS) is an engineering metric describing the user's requirements in terms of the network performance. QOS can be considered as a multi-dimensional metric, including vectors such as:

- throughput (bit-rate)
- bit-error rate
- packet rate
- packet latency
- packet jitter
- packet loss rate
- connection setup delay
- connection setup refusal rate
- security (privacy, authentication)

Applications request a guaranteed QOS from the environment, ensuring that the necessary resources are available for the end-user. Quality-of-service can best be guaranteed on a connection-oriented network based on statistical multiplexing.

The quality-of-service requirements strongly impact the network design; architectures involving multi-dimensional images and image-format data require different QOS than applications involving text or voice. This can be easily seen in the use of 53 byte packets for of ATM/SONET. However, the technologies used in the network design strongly impact what quality-of-service can be delivered; third generation photonic networks can deliver QOS unachievable by conventional electronics. This can be seen from our design of terabit per second networks using femtosecond pulses, where the throughput and packet size can far exceed that obtained from conventional ATM networks.

For any application area, certain issues must be considered regarding the network interconnecting a distributed imaging and visualization environment. These issues include:

- Network must transparently support user and user's applications.
- Must preserve or enhance the interpretive utility of images.
- Paradigms for imaging and visualization must substantially overlap existing practices.

- Must be scalable to network next-generation imaging and visualization technologies.
- Image data acquisition, processing, visualization, and archiving should be considered separately.
- Existing infrastructure (for example, installed cable) should be used where possible.

As our prototype application area we selected distributed imaging and visualization for diagnostic radiology. Image-based procedures are becoming increasing common in medical diagnosis and treatment. It is most practical if the equipment used for these procedures is distributed across the health-care enterprise, from primary-care clinics to tertiary-care centers. Optimally, there would be a distributed imaging and visualization environment, consisting of a heterogeneous array of resources: imagers, high-performance computing, visualization stations, and treatment stations. These resources are interconnected by a high-performance communications network. Each resource is dedicated to its particular function, and offers its functionality to authorized users. As an application area, diagnostic radiology is an excellent model for distributed imaging and visualization, though it differs somewhat from C^{4}I. Diagnostic radiology makes less use of visualization of real-time images as well as making less use of wireless links to the network. Both radiology and C^{4}I make substantial use of archival data; however, this capability is not used as much as it could be due to difficulties in searching for the proper stored image. In both diagnostic radiology and C^{4}I, it is the duty of the network to deliver the quality-of-service required by the application and the end-user.

Image modality	Single image		Complete patient study	
	Image size (pixels^2 × bits)	File size (Mbits)	Images per patient	File size (Mbits)
Computed tomography	$512^2 \times 8$	2.1	100	210
Magnetic resonance	$512^2 \times 8$	2.1	100	210
Ultrasound	$512^2 \times 8$	2.1	50	105
Nuclear medicine	$256^2 \times 16$	1.1	50	53
Plain film (low)	$2000^2 \times 16$	64	10	640
Plain film (high)	$4000^2 \times 16$	256	10	2560

Table 1. Medical image sizes and network data loads. Values are for typical patient imaging requirements. Image sizes are assuming no compression.

Quality-of-service metrics

In collaboration with the UCSD Department of Radiology, we have initiated studies to determine the quality-of-service necessary for diagnostic radiology. Initially, we considered two aspects of the quality-of-service, namely bit-rate and packet latency. To determine these requirements, we need to consider the nature and volume of images transmitted, and the applications requiring these images.

In diagnostic radiology, we consider five principal imaging modalities: plain film diagnostic x-ray, computerized tomography, magnetic resonance imaging, ultrasound, and nuclear medical imaging (which includes gamma cameras and emission computed tomography). In Table 1, the image sizes of these modalities are listed, along with the typical number of images in a patient study and the total study file size. The file sizes listed do not take into account any image compression. In Table 2, the archival storage requirements are listed. The number of patient studies per month is determined by tabulating the number of clinical studies from 1994-1995 and determining the monthly average. The four sites listed (Thornton, Hillcrest,

Women's, and IMG) refer to four different clinical radiology locations of the UCSD Medical Center. Over 6000 Gbits of storage are required per month to archive newly acquired images.

The network must support a variety of distributed applications. These include, but are not limited to instrument control, image acquisition, image processing, archiving, image database search, rendering, and multi-dimensional visualization. All of these applications support the diagnosis, and assist in determining the course of treatment. From these applications, approximations of the required packet latency can be determined. For instance, real-time instrument control, while requiring low bit-rate, also requires very low latency. Distributed interactive visualization requires moderate bit rates, with latencies on the order of 10 ms. Interactive voice and video require lower bit rates then visualization, but also latencies on the order of 10 ms. Archiving and image transfers require the highest bit rates, but also can have latencies on the order of 1 s. Image-guided techniques, for instance telesurgery using force feedback, require latencies on the order of 1 ms, with the force feedback synchronized to the image transmission.

	Patient Studies per Month						
	CT	MR	US	Nuc	DX	Ang	OPC
Thornton	229	97	186	87	1150	150	40
Hillcrest	840	250	625	345	5260	984	1774
Women's	—	—	162	—	320	—	—
IMG	—	—	227	—	593	—	—
Total studies (all sites)	1069	347	1200	432	7323	1134	1814
Data size per study (Mb)	210	210	105	53	640	640	640
Total storage per month (Gb)	224	73	126	23	4291	726	1161
Total storage per month (all image types) (Gb)	**6624**						

Table 2. Data archive storage requirements for UCSD Medical Groups. Data averaged from 1994–1995. Dash (—) indicates no studies performed in particular imaging type at corresponding site. Imaging types: CT–computed tomography, MR–magnetic resonance, US–ultrasound, Nuc–nuclear medicine, DX–diagnostic x-ray film (low resolution), Ang–angio vascular intervention, OPC–out-patient clinic. Sites: Thornton–UCSD Medical Center, Thornton Hospital, La Jolla, Hillcrest–UCSD Medical Center, Hillcrest, Women's–UCSD Women's Imaging Center, Hillcrest, IMG–UCSD Internal Medical Group, La Jolla.

Figure 1 illustrates the quality-of-service requirements for diagnostic radiology applications supported by a distributed imaging and visualization environment. The labels listed at top represent a sampling of the current available technologies, as well as several technologies under development.

Most often, a diagnosis is not made from an isolated image, but from a combination of many elements: sets of images of various modalities (both archived and newly acquired), other examinations and tests, the patient's complaints, and the patient's history. The network must have the capability to transfer entire patient records that consist of both older, archived information and newly acquired information. These patient files will be viewed many times, both for diagnosis and teaching. Therefore, it is apparent that the network load from the visualization of images far exceeds the network load from the original acquisition and archiving of the images. The increased network load that this multi-dimensional visualization and image fusion creates is the subject of current research.

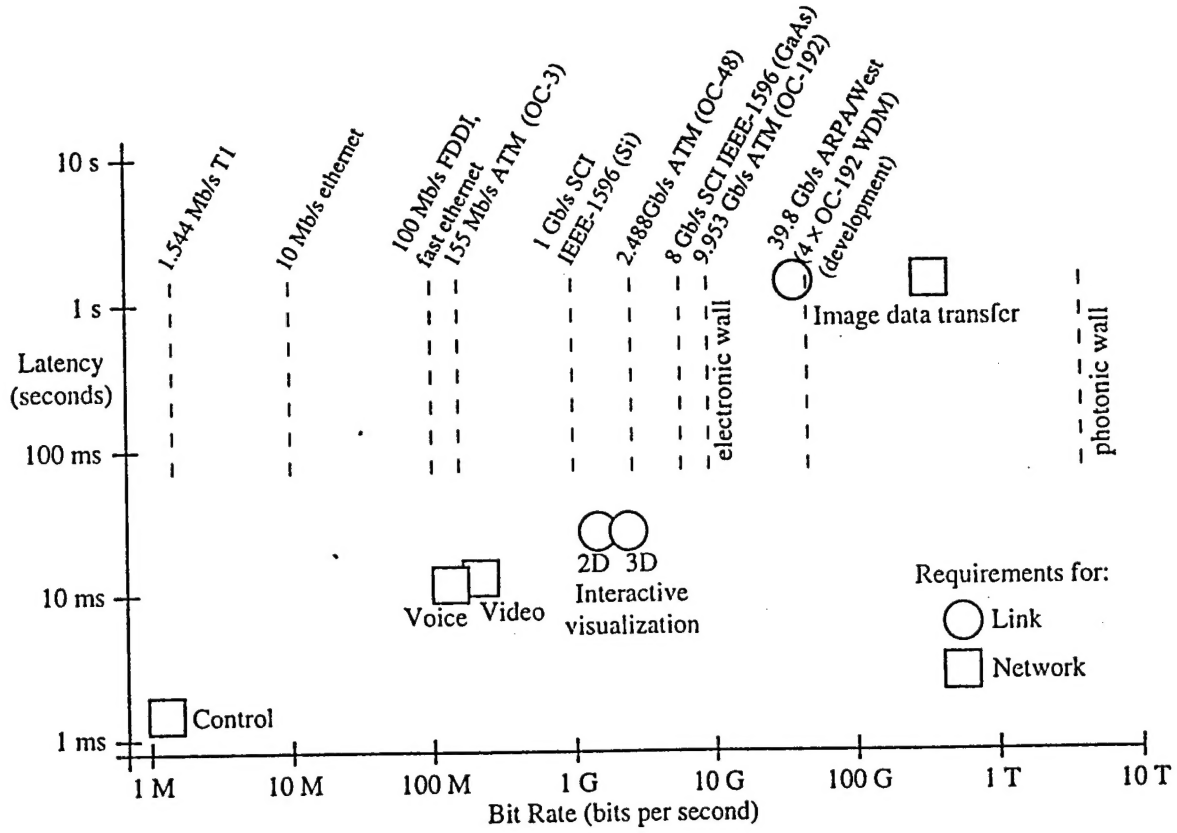

Figure 1. Quality-of-service requirements for typical diagnostic radiology distributed imaging and visualization environment. Labels listed at top represent a sample of the current available technologies, as well as several technologies under development.

Demonstration platform for distributed medical imaging and visualization

To verify the quality-of-service requirements outlined above, and to determine the impact of various schemes to guarantee quality-of-service, we are developing a demonstration platform to support diagnostic radiography in a clinical setting. This platform consists of development in two areas: development of a prototype imaging and visualization environment interconnected by a connection-oriented, statistically multiplexed ATM network; and development of radiologist visualization stations to support diagnoses in a clinical setting.

The distributed imaging and visualization environment is being designed for development in three phases. At the completion of the first phase, we will demonstrate the transmission and interactive visualization of various modalities of medical images over a high performance fiber optic network, and the fusion of these images with an archival digital atlas of human anatomy. The distributed imaging and visualization applications developed for this demonstration will follow closely the existing paradigms used by radiologists.

The first phase demonstration consists of two parts. From UCSD, archival databases of patient histories and images are being developed and interconnected with radiologist visualization stations, clinical review stations, engineering development workstations. and film scanners. Initially, the images and histories stored in these databases will be transferred from the existing diagnostic imaging equipment via magnetic tape, magneto-optical disk, and film scanning. Later, in the second and third development phases, the diagnostic imaging equipment will be directly connected to the network.

The radiologist visualization station is located in a hospital's radiology suite. It consists of eight or more high resolution gray-scale monitors driven by one or more processors, and connected to a workstation for database queries, annotations, and network access. The clinical review station, primarily used in clinics, the emergency rooms, and intensive care units, consists

of two high resolution gray-scale monitors driven by a common processor. We have completed prototypes of clinical review stations and the radiologist visualization station. These workstations are currently being evaluated in clinical environments at the UCSD Medical Center, with test sites at both UCSD Medical Center - Thornron, and UCSD Medical Center - Hillcrest. We also have initiated the development of radiologist visualization stations capable of interactive multidimensional visualization.

From Brown University, digital anatomical textbooks together with a deformable template algorithm for image understanding and interpreting will be integrated into the above platform. The textbooks include digital brain atlases derived from MR density images, CT attenuation density images, and functional PET images. The algorithm transforms the coordinate system of a textbook into that of any patient; it allows fusion of various image modalities, and automatic labels the various structures (white-matter tracts, gray-matter nuclei, Broca's areas, and so forth) of a test image. All the anatomic, histologic, and pharmacologic information in the textbook becomes available in the diagnosis of a patient; the system also provides a quantitative comparison of brain functions between individuals. Later, in the second and third development phases, atlases of other parts of the body will be added.

With this development platform in place, in later phases we will test and evaluate, as they become available, other applications, network algorithms, and photonic interfaces. These will include:

- High data rate photonic interfaces and routers.
- Adaptive image encoding algorithms for network transmission.
- Scheduling algorithms to guarantee required quality-of-service from the network.
- Network security devices and algorithms, including classical and quantum cryptographic key generation.
- Integration of photonic imaging networks with wireless multimedia communications networks (in collaboration with UCSD's Center for Wireless Communications and UCSD/ARO FRI on Wireless Multimedia Communications Networks for the Digital Battlefield).
- Multi-dimensional visualization and image fusion using interactive three-dimensional displays.
- Hierarchical image representation and compression.
- Fusion of images and image-format data.

In addition to the demonstration and test of the above listed items, we will also test the appropriate technologies in a clinical radiology environment, thus generating rapid feedback to the various research groups on their diagnostic efficacy.

Demonstration platform

Our demonstration platform is shown in Figures 2. It consists of three independent subnetworks located at three geographically dispersed sites, interconnected by trunk lines, as well as with other imaging and computing sites on the UCSD campus. We are presently in the process of simulating the performance of our demonstration platform.

The UCSD Medical Center—Thornton is located on the eastern fringe of the UCSD campus, approximately 1 km from the geographic center. Network resources located at Thornton include diagnostic imaging, diagnostic visualization, and research. The UCSD Medical Center—Hillcrest is located approximately 15 km south of the UCSD campus. Network resources located at Hillcrest include diagnostic imaging and visualization. These resources are located at three sites: the Radiology Clinic in the main hospital, the Woman's Imaging Center, and the Magnetic Resonance Institute. The UCSD Department of Electrical and Computer Engineering is located close to the geographic center of campus. Network resources located here include visualization, network control and development, archival database, and photonic interfaces.

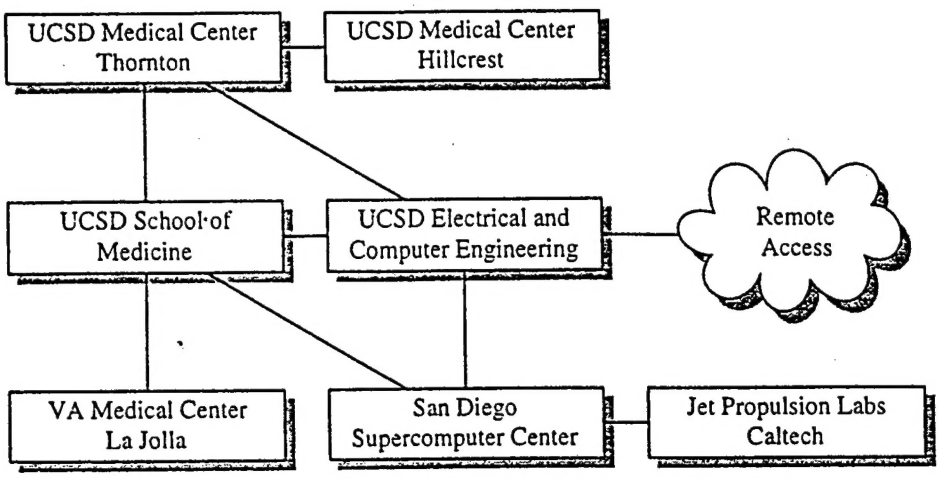

Figure 2. Trunk lines interconnecting various subnetworks in UCSD advanced demonstration platform of a distributed imaging and visualization environment for use in diagnostic medical imaging.

Development of demonstration platform

The development of the demonstration platform will occur in three phases, each of which will build upon an existing baseline architecture. The baseline architecture is being used to develop and prototype databases, clinician interfaces, and diagnostic visualization applications. In addition, all diagnostic imaging equipment identified in these figures currently exists. Resources are interconnected using switched 10 Mbps ethernet. All resources are collocated.

In the first development phase, the collocated resources from our baseline architecture will be interconnected using ATM switching with OC-3 SONET (155.52 Mbps) links from the user end nodes to the ATM switches and OC-12 SONET (622.08 Mbps) links as trunk lines between ATM switches. These switches will be commercial, off-the-shelf. This will enable us to modify the diagnostic imaging and visualization applications so they will operate over a connection-oriented distributed environment.

In the second development phase, we will add additional visualization workstations, image file servers, and database servers, and install this hardware at each clinical site. The trunk lines connecting the clinical sites with other subnetworks will be OC-12 SONET links. A section of the subnetwork located in Electrical and Computer Engineering can be disconnected from the main network, as required, to test and evaluate high-performance photonic technologies using the diagnostic visualization applications currently under development. This will include the terabit photonic links based on spectral domain processing, as developed under the FRI by the Graphics Server Consortium, and transparent photonic network switching fabrics, as developed under other funding. Upon successful evaluation of these technologies, they can be inserted into the full demonstration platform for large-scale evaluation. To ease the demonstration of these photonic devices and systems, a standardized, portable reference hardware architecture is under development.

In the third development phase, we will add additional visualization, database, and network equipment. We will upgrade the database server and the image file server, and add additional computational hardware as required by the various imaging and visualization

algorithms. The third phase of this development represents a fully functional diagnostic radiological imaging and visualization environment.

Image encoding and quality requirements

The proper encoding of the image can reduce the requirements of network. For instance, transport of an image over a lossy, statistically multiplexed network can result in the loss or corruption of a package. To avoid degradation of the image, typically a request is made for re-transmission of the bad packet, with a subsequent degradation in the quality-of-service (i.e., latency). The proper encoding of the packet for progressive transmission can make the transmission immune to the loss of packets, and remove the need for re-transmission. We have studied the encoding of images and image-format data to achieve this goal. We also explored means of using the capabilities of third generation photonic networks to create customized encoding schemes.

One question with the transmission of images over a lossy network involves knowing how much loss is tolerable before the clinical utility of the image is lost. Image quality can be included as another dimension of the quality-of-service metric, and the encoding scheme used to optimize the image quality relative to the bit-error rate and the packet loss rate. Lossy compression can be used as a model for the loss of image quality due to packet loss.

Our research on image data encoding encompassed three areas: the development of spatially-varying compression techniques, the evaluation of lossy compression techniques on the clinical utility of images, and the development of lossless image compression for use over a lossy packet network.

The first project focused on spatially-varying compression techniques. Many classes of images contain some spatial regions which are more important than other regions. Compression methods which are capable of delivering higher reconstruction quality for the important parts are attractive in this situation. For example, in videotelephone sequences, one would like better quality for the face, and in aerial or satellite images some portions of the image may be useless due to cloud obscuration, or are less important because they depict uninhabited territory, etc. For medical images, only a small portion of the image might be diagnostically useful, but the cost of a wrong interpretation is high, so the image quality must be excellent in the medically relevant portion.

In this work, we devised algorithms which are capable of delivering lossless compression within the region-of-interest (ROI), and lossy compression elsewhere in the image. We call such methods "lossless ROI compression." With the goal of truly lossless coding of a region, quite different techniques are needed compared with the goal of providing higher (but still lossy) quality. Powerful methods for lossy coding may perhaps be applicable only in conjunction with a lossless coder for the regional residual image. One of our algorithms is based on lossless coding with the S-transform, and two are based on lossy wavelet zerotree coding for the non-ROI region, together with either pixel-domain or transform-domain coding of the regional residual within the ROI.

We found that the results depended on several factors, including the size and shape of the ROI, and the desired background PSNR. For almost all background PSNRs and larger ROI sizes of interest, a wavelet zerotree coder followed by lossless encoding of the residual with an S+P transform gave the best results. For very small ROIs or very high values of background PSNR, simpler methods using wavelet zerotree coding followed by arithmetic or Lempel-Ziv coding became competitive with the wavelet/S+P method. For these simpler methods, the optimal division of the encoding work between the initial wavelet coder and the final entropy coder was found to depend on the background PSNR chosen.

The second project was aimed at evaluating the effects of lossy image compression on digitized mammograms. Conventional mammography machines involve analog films, which are

viewed on a lightbox. The substitution of digital representations for analog images provides access to methods for digital storage and transmission and enables the use of a variety of digital image processing techniques, including enhancement and computer assisted screening and diagnosis. In the mid-1990's, several manufacturers have developed digital-acquisition mammography machines which have not yet been granted market approval from the Food and Drug Administration. A switch to this technology will bring the question of digital image compression to the forefront of radiology.

While lossy compression can further improve the efficiency of transmission and storage and can ease subsequent image processing, digitization and digital acquisition and lossy compression do alter an image from its traditional form, and hence it becomes important that any such alteration be shown to improve or at least not damage the utility of the image in a screening or diagnostic application. One approach to demonstrating in a quantifiable manner that a specific image mode is at least equal to another is by clinical experiment simulating ordinary practice and suitable statistical analysis. In this research, we developed a general protocol for performing such a verification, and conducted such a clinical experiment designed to show that 12 bpp digital mammograms compressed in a lossy fashion to 0.15 bpp using an embedded wavelet coding scheme result in no statistically significant differences from the analog or digital originals.

The clinical experiment involved 57 patient studies and 6 radiologists. Images were viewed on hardcopy film on an alternator by judges in a manner that simulates ordinary screening and diagnostic practice as closely as possible, although patient histories and other image modalities were not provided. Two views were provided of each breast (CC and MLO), so four views were seen simultaneously for each patient. Each of the judges viewed all the images in an appropriately randomized order over the course of nine sessions. Two sessions were held every other week, with a week off in between. A clear overlay was provided for the judge to mark on the image without leaving a visible trace. For each image, the judge either indicated that the image is normal, or, if something was detected, had an assistant fill out a detailed Observer Form using the American College of Radiology (ACR) Standardized Lexicon by circling the appropriate answers or filling in blanks as directed. The initial statistical analysis focused on the management decisions made by the radiologists, and on the subjective scores assigned to the images. Current statistcial analysis is aimed at evaluating the detection sensitivity.

The primary conclusion from the initial data and analysis is that variabilities among judges exceed by a considerable amount, in their main effects and interactions, the variability in performance that owes to imaging modality or compression within very broad limits. In other words, the differences among analog, digital, and lossy compressed images are in the noise of the differences among radiologists, and are therefore more difficult to evaluate. Additional data has been gathered from an additional six radiologists at another university. This work was conducted primarily at Stanford University with the support of the Army Medical Research and Materiel Command.

The third project involved lossless compression over a lossy packet network. The goal is to compress an image and packetize it such that if all packets are received, the reconstructed image will be identical to the original. If some packets are lost, the reconstruction should still be reasonably high quality. This work is in contrast to other schemes of this type which focus on lossy compression, that is, even when no packets are lost, the reconstructed image is still lossy.

One algorithm we developed uses simple linear prediction to decorrelate the image. The prediction residuals are compressed using Huffman coding. The encoded image is then placed into 48 byte ATM packets. Each packet begins with the row and column position of the first pixel in the packet. The actual value of the first pixel is also included. This becomes the seed value for the prediction sequence within the packet. By including this "header" information, each packet becomes self contained (independently reconstruct able). Additionally, each packet

contains equal importance. In the event of lost packets, the missing pixel values are estimated using linear interpolation.

Our second scheme uses subband coding to decorrelate the image. The sequential transform, in combination with prediction, is performed on both the rows and columns of the image. Each subband is Huffman coded. Each ATM packet again begins with the row and column position of the starting pixel. Thus the scheme is tolerant of packets being received out of order. The sequence in which the encoded image is packetized follows the parent/descendant order of subband coefficients. Thereby each packet carries equal weight, on average. In the event of a lost packet, the missing encoded values are replaced by zeros prior to performing the inverse transform.

Both methods were evaluated using two 256x256, 8 bpp, MR brain images. The linear prediction resulted in a compression rate of approximately 5.3 bpp for the scan pattern of pixel width 2 and approximately 5.2 bpp for the scan patterns of widths 4 and 6. The peak signal-to-noise-ratio resulting after reconstruction from a single lost packet was approximately 59 dB for the scan patterns of width 2 and 4 and 57 dB for the width of 6. The reconstructed images were visually indistinguishable from the original images.

The subband decomposition methods did not perform as well as the pixel-domain linear prediction methods. Although some of the subband methods used provided greater compression than the linear prediction techniques, these methods could not be made to be self-contained within the packet. And in this case, the loss of a single packet could produce errors which propagated over a large region and were visually objectionable. The other subband methods (involving no prediction and only one or two levels of decomposition) could be packetized in a self-contained way; however, these methods provided no compression advantage over the simpler pixel-domain linear prediction.

Transparent photonic switching networks

In coordination with the research we are conducting under this grant, we are investigating various methods of developing transparent optical switching fabrics. We are striving to use the results of these efforts as the backbone of more extensive photonic networks using spectral domain processing for data encoding. We have undertaken two separate approaches. In the first, we developed a cascaded optical delay (COD) multiplex using commercial-off-the-shelf components. The present embodiment of the COD is based on fiber optic and integrated optic components. In the second, we developed switching fabric using a transparent optical multistage interconnect network (TOMIN), based on birefringent computer generated holograms technology being developed at UCSD which forms an 8×8 nonblocking interconnection network. The present embodiment of the TOMIN is based on free-space optics.

Transparent Optical Multistage Interconnection Network for Image Transmission

Image transmission between large numbers of I/O ports, requiring switching of ultra-high bandwidths, can be performed using optical multistage interconnection networks (MIN). Polarization based switching has been proposed for 'free-space' MIN for switching and multiprocessor interconnections. We have designed, fabricated and tested a 'folded' optical MIN system that permits switching high-speed signals between multiple input and output nodes using a simple and compact arrangement of diffractive optical and polarization rotation elements. In this system, optical routing is performed using bypass-exchange switches built of polarization sensitive birefringent computer generated holograms (BCGH) combined with electrically addressed polarization rotation devices. This transparent and scalable system can switch multiple high bandwidth communication lines or permit memory access and multiprocessor interconnections.

BCGH, which are diffractive optical elements that have independent impulse responses for two orthogonal linear polarizations, and ferroelectric liquid crystal (FLC) polarization rotators can be used to implement bypass-exchange switches. Such switches accept two independent input channels, which can be exchanged depending on the state of the polarization rotator within the switch. In order to reduce the potential linear cross-talk (ε) of this design we have implemented our optical MIN using dilated bypass-exchange switches (DBES), which cluster together four regular bypass-exchange switches. This switch allows for filtering of the linear cross-talk noise with only the small second order (ε^2) crosstalk remaining.

By combining several DBES switches into layers, together with simple optics to create a desired interconnection pattern, a larger network can be constructed. For example, to connect eight input channels to any combination of eight output channels requires only three layers, where each layer is comprised of four DBES (two inputs per switch). For our system demonstration a Banyan interconnection pattern is implemented using off-axis Fresnel lenslets fabricated using multi-layer computer generated holograms (CGH). The configuration of the system exchange pattern is done by simultaneously setting the states of the FLC polarization rotators within each of the switches.

Another advantage of using the DBES for optical switching is its symmetric design. By 'folding' the switch, with the use of a mirror, the functionality of the four regular bypass-exchange switches can be performed by only two such switches. This folded arrangement allows for like, i.e. BCGH and FLC, elements to be grouped into 2-D arrays. Therefore, a single bypass exchange switch, which performs switching between two inputs and outputs, can be implemented using 2×2 arrays. Incorporating an array of CGH elements to implement a specific network interconnection architecture and increasing the size of the BCGH and FLC arrays performs multi-channel interconnections. For example, for a network that switches between eight input and output channels we use 8×6 arrays of CGH, BCGH and FLC elements (see Fig. 3a).

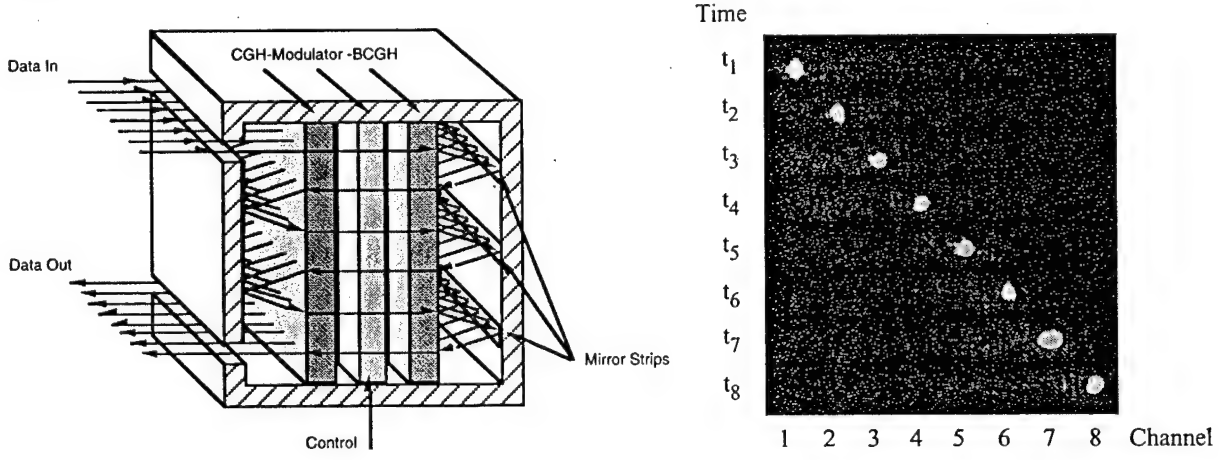

Figure 3. (a) Folded MIN system layout showing 2-D arrays of CGH, FLC, BCGH elements and micro-mirrors. Each round trip (from left-side to left-side) completes a single dilated bypass exchange switch (2×2 functionality). Three passes (as in the above system) allows for 8×8 interconnection. (b) CCD images of outputs to eight channels from a single channel input shows negligible cross-talk, average of 78:1, between channels.

Our demonstration system uses global control of switching elements (i.e. state of polarization rotators for each DBES) using a Gated Hold Protocol which is based upon fixed message size and supports blocking networks. This protocol serves all non-blocked requests, and resolves blocking situations by signaling and coordinating the sources. Since global control of this system

is performed electronically, existing electronic networks, performing low-priority or small bandwidth communication operations, can be used for command and control for an overlaid high-speed optical MIN.

Cross-talk due to unwanted diffraction orders can be filtered out of the system by using strip mirrors or micro-mirrors that allow unwanted optical signals to propagate out of the folded system (see Fig. 3a). Initial testing of a single dilated bypass exchange switch (i.e. 2×2 system) using BCGH, CGH and FLC arrays has shown cross-talk of less than 1:200. In Fig. 3b we show CCD images of the outputs to eight channels (i.e. 8×8 system) using a single input channel. Average cross talk between output channels is 1:78. Testing of the system using a high-speed signal generated from an acousto-optic (AO) cell light modulator indicates that the optical MIN system is transparent, i.e. signal-to-noise of is independent of signal bandwidth.

The reconfiguration of the network is currently limited by the speed of the FLC device. However, we are developing a PLZT based polarization rotator array having much faster response times. Advances in fiber amplifiers and polarization compensation in a single mode fiber may enable utilization of polarization dependent all-optical switches using optical fiber input and outputs.

Incoherent phase noise from optical multi-path

In transparent photonic networks it is possibly to get multipath noise caused by the imperfections in switching. When these signals travel over vastly different path lengths, it is believed that the signals add in intensity (incoherently), and have a minimum impact on the error rate. We have found that these signals can add in field, producing incoherent phase noise, which can have a significant impact on the error rate.

We experimentally evaluated the impact of incoherent phase noise in a photonic network by modeling the network by a fiber optic Sagnac interferometer. The recirculating loop in the interferometer had both an attenuator and polarization rotator so the intensity and state-of-polarization of the loop signal could be adjusted relative to the pass-through signal. Various lengths of optical fiber (ranging from 10 m top 4 km) were placed in the loop to determine the effects of coherence on the phase noise. The input signal to the interferometer was an ASK modulated laser diode operating between 700 Mbps and 1.1 Gbps, with a coherence length on the order of 1 cm.

We have measured the bit-error rate of the interferometer for the case when the loop signal is orthogonally polarized to the pass-through signal, and for the case that the loop signal has the same state-of-polarization as the pass-through signal. For the case of orthoganally polarization, the experimental data agrees with a simple theory that assumes incoherent intensity addition. For the case of the same state-of-polarization, we observed the interference between the loop signal and the pass-through signal, at loop lengths of up to 4 km. This was seen from the eye diagram, which showed a contraction of the eye, with increased jitter, and from bit-error rate measurements. The bit error rate degraded by seven orders of magnitude as compared to the orthoganally polarized case (from a value of 10^{-10} for orthogonal polarization to 10^{-3} for the same-state-of-polarization).

Also, we evaluated incoherent phase noise using an optical fiber Mach-Zehnder interferometer. The Mach-Zehnder interferometer has the advantage of being easier to develop numerical models for. The Mach-Zehnder interferometer consists of a 3dB coupler to split the input data signal. One path is delayed with respect to the other, pass through, data signal and the two signals are re-combined by a second 3dB coupler. This combined signal is detected by a high-speed receiver and the signal compared to the input signal by a bit error rate tester. Additionally, the polarization state of one path is set parallel to the other to provide maximum interference. The recombined bits are set such that the data bits are aligned with respect to each other. A polarization maintaining optical attenuator is used in the delayed path to vary the data

signal to interference signal ratio and the resulting bit error rate measured for a pseudo-random bit stream input. Figure 4 shows results of the bit error rate curve for a 2km difference delay path and a bit rate of about 1Gbps.

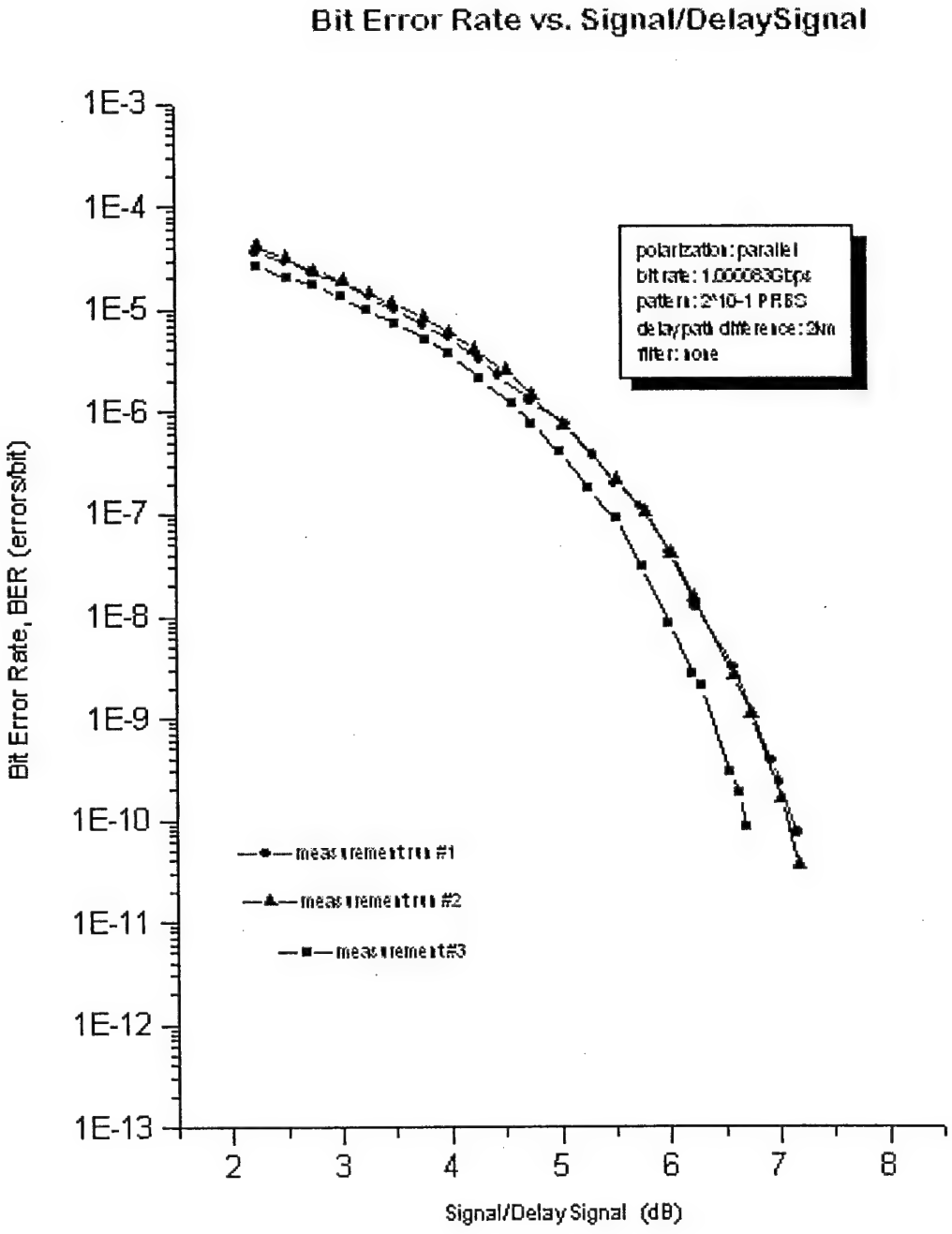

Fig. 4. BER experimental results for a channel modeled by asymmetric Mach-Zehnder Interferometer to emulate incoherent multipath noise.

The curves shown are very smooth and repeatable. The 2km path length difference is well over four orders of magnitude greater than the coherence length of the transmitter, setting the interference effect well into the incoherent region. It was found that when the path length difference was near zero, where the signals are highly coherent, mechanical vibration within the fiber due to environmental influences have a great effect on the stability of the bit error rate curve. Although there is a slight variation, the error rate remains relatively constant between the three curves for the incoherent case. Additionally, every error measured has been found to be a 1 to 0 error rather than a 0 to 1 error. This is significant since errors due to a 1 bit interfering with a 1 bit will always cause only 1 to 0 errors. Thus our hypothesis that intensity noise due to interference between the two signals is significantly greater than other noise sources is supported.

Continuing research is investigating the theoretical BER results for a two-signal interferometer and a computer simulated model of the experimental work. Assuming a gaussian distributed phase fluctuation in a monochromatic constant amplitude input data signal, the output intensity distribution is determined from a histrogram of multiple input phase differences. The histograms in Figure 5 show the distribution of the results for 2000 trials at three different ratios of delayed signal to data signal.

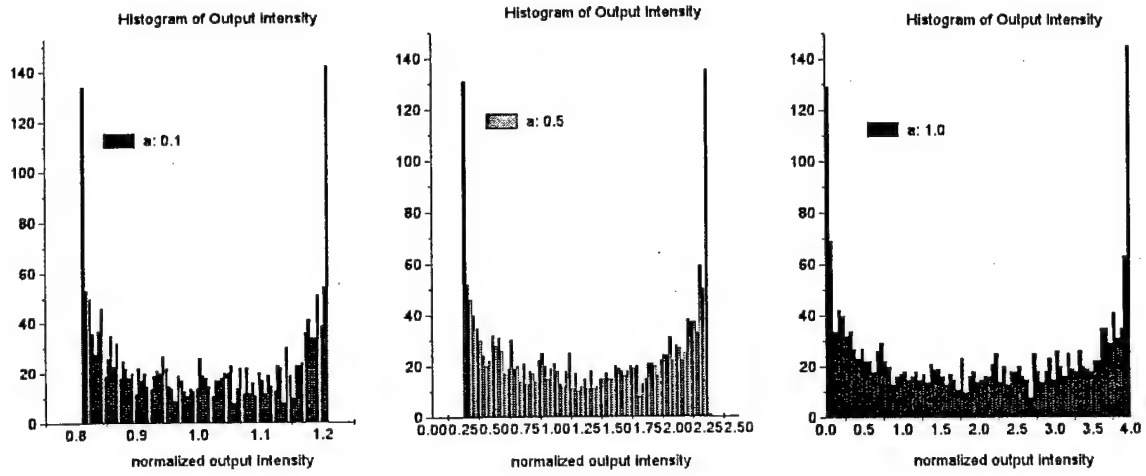

Fig. 5. Histogram of output intensities for simulation of asymmetric Mach-Zehnder fiber interferometer.

As the ratio of the signals increases, the probability of the output intensity reaching below the decision threshold also increases. Previous results have shown that the BER curve for orthogonal polarization indeed follows the theory. Errors occur mainly when bit overlap results in a 1 on a 1 or a 1 on a 0. By combining the theoretical results from the orthogonal case and those above, an accurate model of the effects of phase-induced interferometric intensity noise on the BER of a fiber optic system may be developed.

Four-wave mixing noise

Four-wave mixing (FWM) noise is a nonlinear process, occurring because of the third-order nonlinear susceptibility in optical fibers, and causing signals at various frequencies to interfere between each other and give rise to signals at different frequencies. The process manifests itself in two effects: it transfers power from the signal channels to the FWM terms depleting the power of the signals; when the newly generated FWM terms fall within a signal channel they interfere with the signal generating crosstalk.

One possible way of reducing the FWM noise is to de-couple the wavelength channels in time, meaning that not all the wavelength channels overlap in time. This gives a reduction in the

number of FWM terms (and the noise associated with it) appearing in the system. The decoupling can be done artificially by means of sparse coding; an environment where it occurs naturally are optical networks with channel utilization factor less than one. We have investigated two network models; a circuit-switched model, where the utilization factor gives the probability that a wavelength channel is present on a certain link; concurrently, we have investigated a packet-switched model where the utilization factor for a certain wavelength gives the probability that a packet at that wavelength is present at a certain time. Evaluating all cases of overlapping for a utilization factor less than one, we have derived the mean reduction in FWM terms for both models. The reduction was evaluated in terms of reduction in the total number of depletion and crosstalk terms, and also reduction in the number of dominant or phase-matched depletion and crosstalk terms. Both expressions indicate that for a realistic utilization factor of 0.8 a natural reduction in excess of 3dB is achievable.

The obtained expressions are in terms of average values over all possible sets of wavelengths. As a further step, we plan to explore the possibility of modifying the protocols to incorporate only certain sets of wavelengths, for which reduction markedly better than the average one can be obtained. In doing so, we have discovered certain linear transformations, for which the FWM is invariant. We plan to design protocols in terms of optimal sets of wavelengths, which will allow even further reduction of the FWM terms and to investigate the impact of these new protocols on the overall performance of the optical networks.

B. Nonlinear Spectral Domain Processing for Multiplexing/Demultiplexing

The bandwidth and the efficiency of fiber optic communication systems exceed these of electrical cable systems. However, presently, we are far from realizing the potential performance of optical networks. Electronic devices and systems connected to optical networks may reach bit-rates on the order of 1-10 Gb/s. In contrast, the maximum bit-rate of a photonic network may exceed 1 Tb/s. The 2-3 order-of-magnitude mismatch between fiber and device capacity can be used to increase the speed, security, and reliability in the data transmission. To implement these network functionalities, it will be necessary to construct an all-optical pre-processor at the transmitter and a post-processor at the receiver which will perform multiplexing and demultiplexing, respectively. The multiplexer performing space-to-time transformation will combine relatively slow parallel electronic channels into an ultrahigh bandwidth serial fiber optic channel, whereas the demultiplexer will perform the inverse time-to-space transformation for electronic detection. For efficient bandwidth utilization, these processors need to be operated at rates determined by the width of the optical pulses. There exist various techniques to implement the multiplexer. For example, pulse shaping devices have been used to modify the temporal shape of a femtosecond optical pulse by temporal spectral filtering.

The work at UCSD has been initially focused on real-time holographic method that allows parallel-to-serial (i.e., space-to-time) optical signal conversion by encoding spatial frequency spectrum of the parallel optical signals. This multiplexer/demultiplexer processors are using spectral domain four-wave mixing in photorefractive crystals of lithium niobate. However, these implementations in photorefractive crystals do not meet the speed requirements of ultrahigh bandwidth communication systems. Research on development of fast photorefractive materials is carried out by the Purdue University team, while we are continuing the analyses of the performance characteristics of such four-wave mixing processors. Simultaneously, we initiated an alternative approach to satisfy such high speed requirement. We have developed and experimentally demonstrated an all-optical post-processor that implements time-to-space demultiplexing at femtosecond rates by exploiting spectral domain nonlinear three-wave mixing in LBO crystal. In the following, we summarized the principle and the experimental demonstrations of the optical processors for multiplexing and demultiplexing of optical signals for ultrahigh bandwidth communication.

Optical multiplexer by space/time holographic 4-wave mixing of spatial/temporal frequency

Our approach for parallel-to-serial optical data conversion (multiplexer) is based on combining optical information processing that uses spectral domain wave mixing (holography) with that of conventional spatial Fourier transform wave mixing (holography). The all-optical parallel-to-serial conversion processor is shown schematically in Fig. 6a. The processor consists of two independent optical channels for carrying the temporal and the spatial information. The temporal information carrying channel consists of a pair of gratings and a 4-F lens arrangement. The incident pulses are transformed by the input grating and the first lens into temporal frequency spectrum distribution in space of the focal plane, while the second lens and the output grating are performing the inverse transformation of the temporal spectrum distribution back to the time domain. The spatial information carrying channel is a simple optical spatial Fourier transform arrangement consisting of the input image plane and a beamsplitter to share the second lens of the temporal channel. To achieve interaction between the temporal and spatial frequencies spectrum information we use a real time holographic material in a four-wave mixing arrangement. For our initial experiment we used a 1 mm thick photorefractive crystal of $LiNbO_3$. A 1-D binary input image (or a 1-D spatial light modulator) is illuminated by a monochromatic optical source, Fourier transformed into the plane of the real-time four wave mixing material where it interferes with the plane reference wave. The interference pattern via

the photorefractive effect causes recording of a spatial Fourier transform hologram. The recorded spatial Fourier transform hologram is reconstructed by the temporal frequency spectrum of a femtosecond pulse with a center wavelength close to that of the monochromatic source used for the recording process. Note, that the temporal frequency spectrum is spatially distributed along the transverse coordinate of the hologram plane. Therefore, the diffracted temporal frequency spectrum is modulated by the spatial frequency spectrum of the recorded hologram. Upon transmission through the second lens and the output grating, the diffracted temporal frequency spectrum results in a sequence of short pulses which exhibit one-to-one correspondence with the 1-D spatial distribution in the input image. Note, that the resultant sequence of temporal pulses is carried by a single beam which can be easily coupled into an optical fiber link. For decoding of the temporal information at the receiver node we also need to transmit a single reference pulse.

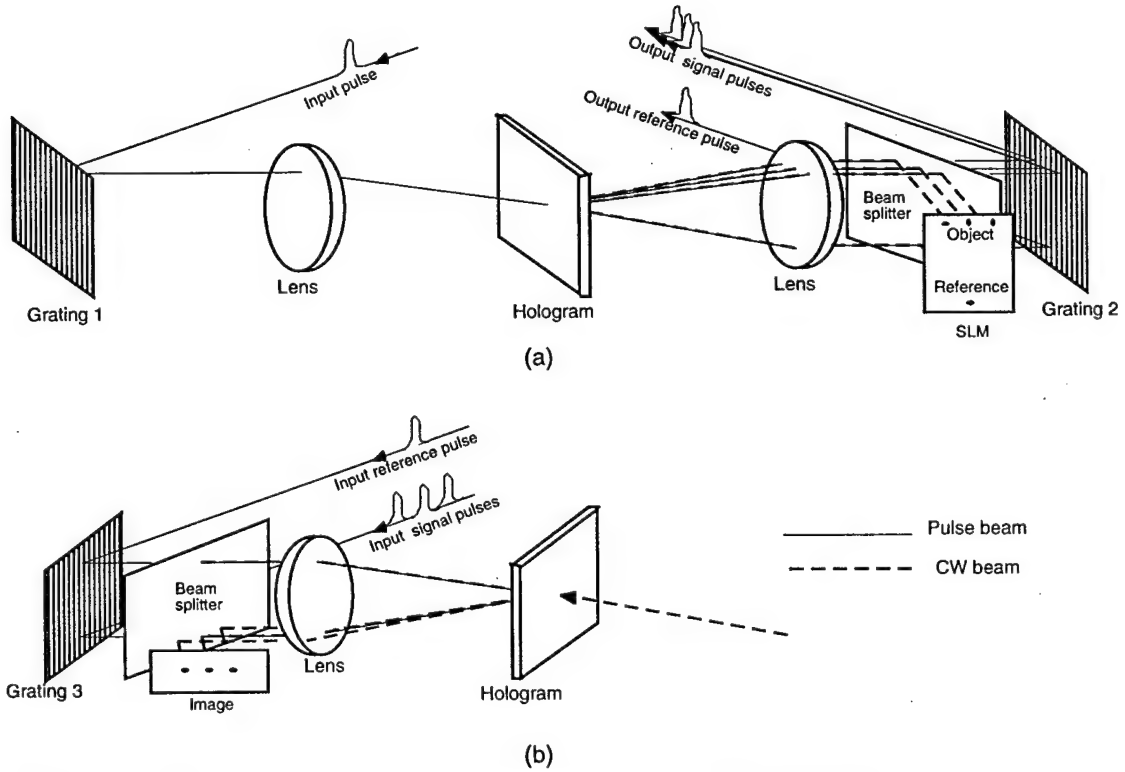

Fig. 6 Schematic diagram of optical processors for (a) parallel-to-serial conversion and (b) serial-to-parallel conversion

At the receiver node we need to perform an inverse serial-to-parallel transformation. Such a transformation can be utilized with spectral holography of the sequence of temporal pulses and a reference pulse as shown schematically in Fig. 6b. The recorded spectral hologram is reconstructed using a monochromatic plane wave resulting in a diffracted wave that is modulated by the spatial frequencies of the spectral hologram. Upon transmission through the spatial Fourier transform lens, the diffracted wave results in a 1-D image which exhibit one-to-one correspondence with the sequence of the incident short pulses. Therefore, transmission of images and image-format data can be achieved.

In the experiments we used 150 fsec optical pulses at a wavelength of 480nm, generated from a mode-locked Ti:Sapphire laser and a frequency-doubling BBO crystal. To satisfy Bragg matching conditions required by volume holography in a 1 mm thick $LiNbO_3$ photorefractive crystal, we used a wavelength of 488nm line from a monochromatic CW argon laser. During

these experiments the output pulses from the system shown in Fig. 6a were transmitted directly to the input of the system shown in Fig. 6b. In order to assure that there was no spatial information carried by the transmitted signal pulses, spatial filtering was performed to eliminate higher spatial frequencies. Alternatively, the output and the reference pulses can be transmitted through two identical optical fibers or through a single fiber using polarization multiplexing. A 1-D binary input image (see Fig.6a) was used in our experiments for parallel-to-serial and serial-to-parallel conversion (see Fig. 6b) employing the processors shown in Fig. 6a and 6b, respectively. The transmitted image in Fig. 7b shows exact correspondence to the original image in Fig. 7a.

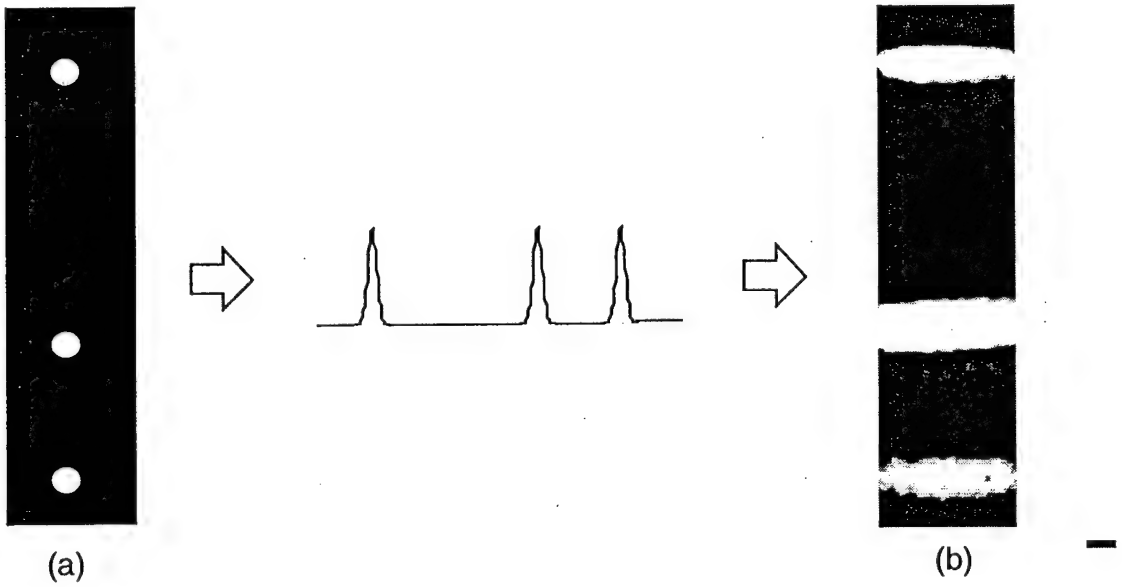

Fig. 7. Experimental results of image transmission using parallel-to-serial and serial-to-parallel conversion (a) the original and (b) the received 1-D image

Optical demultiplexing by nonlinear three-wave mixing of spatial/temporal frequency spectrum

Our demultiplexer system is based on nonlinear three-wave mixing in a LBO crystal. The two input waves are the spectral decomposition waves (SDW) of a shaped pulse and the reference pulse (see Fig. 8a). The nonlinear interaction between the two beam's SDW results in generating a quasimonochromatic second harmonic wave. The frequency of the second harmonic fields is twice the center frequency of the incident fields. Furthermore, the generated second harmonic fields contain spatial frequencies determined by the time delay between the reference pulse and the different temporal features of the shaped pulse. Therefore, a 1-D spatial Fourier transform of the second harmonic fields will produce a 1-D spatial image equivalent to the temporal cross-correlation function between the reference and the shaped pulses. When the reference pulse is much shorter than the information carrying shaped pulse, the autocorrelation image can be approximated by the spatial image of the shaped pulse itself, thus implementing the desired demultiplexing at femtosecond rates.

The optical setup for high speed pulse imaging is depicted in Fig. 8a where 200 femtosecond pulses at wavelength 920nm are generated from a mode-locked Ti:Sapphire Laser. The laser output is split into two beams, one to be used as a reference beam and the other sent into a pulse shaping device to create a shaped pulse. The shaped pulse and the reference pulse beams were then introduced into the pulse imaging system of Fig. 8a. Both beams are spatially

expanded and collimated to produce a large illumination area on the gratings, providing a wider time window for time-to-space conversion. The two metallic blazed gratings of 600 line/mm gratings and the two incident beams are arranged vertically in order to obtain the necessary spectrum inversion of the corresponding SDW. Such arrangement introduces a vertical spatial carrier frequency between the SDWs of the two input pulse beams in the Fourier transform plane. These two beams are then introduced into the LBO nonlinear crystal where under the condition of noncollinear phase matching, the second harmonic field will be generated and propagate in a bisector direction which is parallel to the optical axis. A horizontal slit and a narrowband filter is placed behind the crystal to filter out the light at the fundamental frequency of the two input beams. A second lens is used to perform a spatial Fourier transform of the second harmonic quasimonochromatic field, producing an image that was detected by a CCD camera.

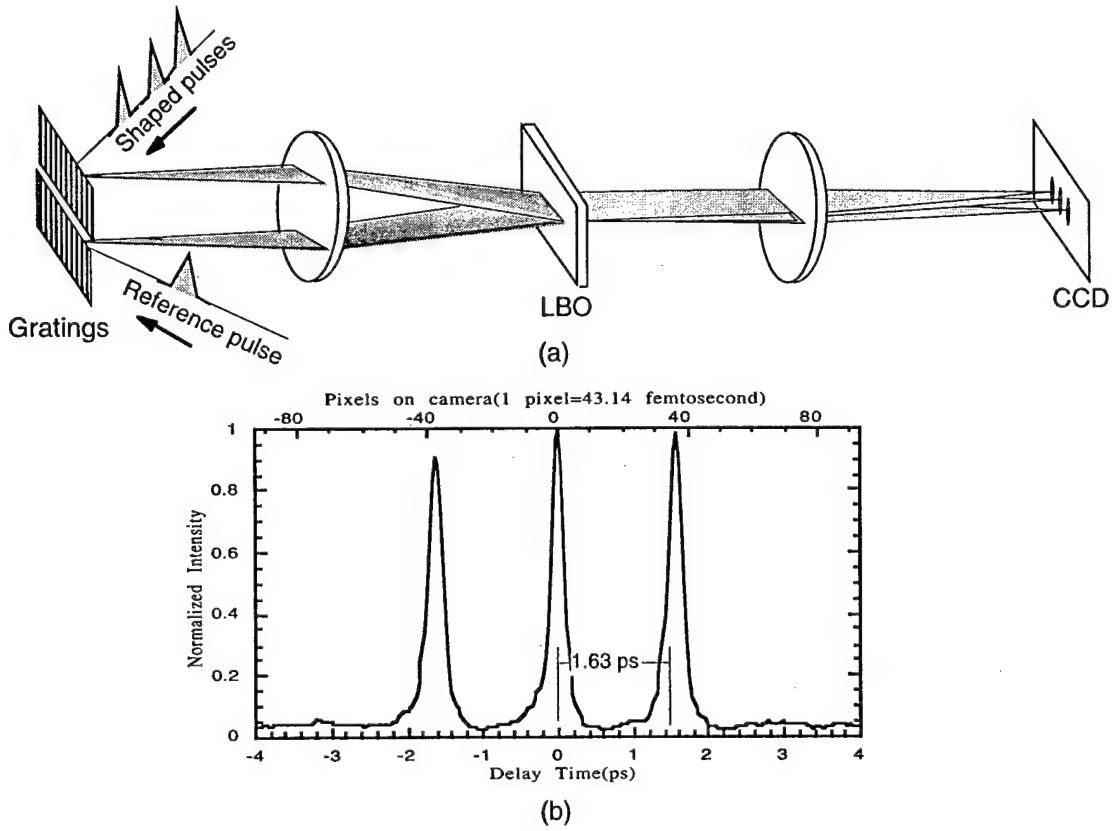

Fig. 8 (a) Optical setup for pulse imaging (b) Intensity profile measured from a shaped pulse that consists of three pulses separated by 1.63 picoseconds

In our experiments we first calibrate the system by varying the time delay between two transform limited 200 fsec pulses. The spatial distance between the two adjacent pixels of the CCD camera corresponds to 43.14 femtoseconds in time scale. Next we use a pulse shaping device to produce a shaped pulse beam. In principle, the temporal shape of the pulse obtained from the pulse shaping device is proportional to the temporal Fourier transform of the spectral filter transmittance function. For example, when the spectral filter is implemented by a simple grating, the resultant shaped pulse will consist of a sequence of equally spaces single pulses each with different amplitude, depending on the specific grating structure. In our experiments we use a sinusoidal phase grating to generate the shaped pulse. This pulse is introduced into our pulse imaging system shown in Fig. 8a. The resultant shaped pulse image consists of 3 pulses

separated by 1.63 picoseconds (see Fig. 8b). The measurement results are found to be in good agreement with the calculated pulse shape obtained for the sinusoidal phase grating.

Analysis of spatio/temporal converters for all-optical communication links

In this research, a parallel-to-serial transmitter and a serial-to-parallel receiver are analyzed for an optical communication link, without the limiting assumption that the bandwidth of the pulse is very small when compared to the optical carrier frequency. The analysis of the parallel-to-serial transmitter and serial-to-parallel receiver is carried out in the mixed temporal/spatial frequency domain. A real-time hologram by four-wave mixing (4WM) of CW spatial frequencies and temporal frequencies from ultrashort pulsed waves is employed. The transfer of information from the spatial domain to the temporal domain, and vice-versa, is accomplished through the interchangeability of the spatial frequencies and the temporal frequencies' information for signals in spatial and temporal domains, respectively.

The parallel-to-serial transmitter is based on real-time four-wave mixing in frequency domain. The temporal frequency spectrum of an incident ultrashort pulse is modulated by a sequence of linear phase functions created by the interference of a signal sequence of CW point sources and a reference point source from the spatial channel. The resultant temporal channel output is a sequence of ultrashort pulses shifted in the time domain according to the slope of the corresponding linear phase function from the spatial frequency domain.

To analyze the temporal output of the resulting pulses, we make several assumptions: frequency ω is replaced by $\omega_0+\delta\omega$ along with the assumption that $\delta\omega<<\omega_0$, a Gaussian pulse envelope function is assumed, and we neglect some edge effects in the aperture function of the output grating. Under these assumptions, the output of the processor is given by

$$s_0(x";t)=\sum_n A_n \exp[j\omega_o t]w"[-x"+n\Delta"]\frac{1}{\sqrt[4]{1+\xi^2 n^2}}\exp\left[j\frac{\tan^{-1}(\xi n)}{2}\right]\exp\left[-\frac{t_n^2}{2\tau^2}\frac{1+j\xi n}{1+\xi^2 n^2}\right], \quad (1)$$

where $t_n \equiv t-t_0-n\dfrac{\Delta''}{c}$ is the time delay of the n-th pulse or bit encoded (with A_n the binary bit information), and we define $\Delta'' \equiv \dfrac{\alpha\omega_w\Delta}{\omega_o}$, and $\xi \equiv \dfrac{2\Delta''}{c\omega_o\tau^2}$, where $\alpha=\sin(\theta)$ with θ being the inclination angle between the incident wave and the reflection grating, ω_w is the frequency of the CW source, ω_0 is the center frequency of the short pulse with time constant τ, Δ is the spatial separation between channels in the spatial domain, and c is the speed of light. Eq. 1 describes a sequence of temporal pulses, each with a slightly shifted aperture position, with a different relative phase and a broadened pulse-width since these pulses are no longer transform limited (i.e., chirped). The amount of chirp increases as n increases, with a positive chirp for n positive and negative for n negative.

The anticipated chirping of the output pulses from the parallel-to-serial transmitter were verified experimentally by cross-correlation measurements. In this experiment, a short pulse from a Coherent Mira 900 laser (λ_o=0.92 μm and τ=93 fs, assuming a Gaussian pulse) is split by a beam splitter into two arms. One arm includes a pulse shaper that simulates the transmitter, and the second is an equal length delay arm. The linear phase functions in the spectral plane were generated by amplitude Ronchi gratings, whose Fourier series decomposition reveals that the 0 and the ±1 orders are predominant. Therefore, the output signal for each grating consisted of three strong pulses, the original transform limited pulse and the two signal pulses, one preceding and one trailing the transform limited pulse. One of these pulses is up chirped and the second down chirped. This output was analyzed by an intensity cross-correlation (Inrad Auto-correlator

514-BX modified for cross-correlation measurements) with the original transform limited pulse in the delay arm.

The Full Width at Half Maximum (FWHM) value was used as a basis for comparison between the calculated and measured result. Three different Ronchi gratings of varying frequencies, i.e. 20, 28, and 39 lp/mm, were used as the spectral filters in the pulse shaper.

The performance of the 4 wave mixing receiver is shown analytically to be unaffected by the chirped pulses when transmitted through an idealized distortionless medium, for data recovery in the spatial domain. In practice, these signal pulses will be transmitted through an optical fiber possessing dispersion and random phase variations due to ambient conditions, thereby affecting the perfect signal recovery in the spatial domain at the receiver. To overcome the fiber dispersion effect, we send the reference pulse along with the data pulses. Thus the phase distortion of the channel, sampled by the reference pulse, is compensated at the receiver via phase conjugation process, when interfered with the data pulses.

Again invoking the Gaussian pulse assumption, the resultant diffracted field in the serial-to-parallel receiver is

$$h\left(x^{\dagger}\right)=\sum_{n}A_{n}\exp\left(-\frac{\alpha^{2}}{4\tau^{2}\omega_{o}^{2}}\left(\frac{x^{\dagger}}{\lambda_{r}}+\frac{n\Delta''}{\alpha\lambda_{o}}\right)^{2}\right), \tag{2}$$

which describes a collection of Gaussian spots separated in space. The location of the peak of each diffraction order is at $x^{\dagger}=-n\Delta\frac{\lambda_{r}}{\lambda_{w}}$, where λ_W is the CW wavelength used to write the phase function in the transmitter, and λ_r is the CW wavelength used to read out the interference of the pulses. The presence of a signal at a diffraction order location n is determined by the information bit A_n. A linear detector array placed at the output plane reads the information packet, with detector response time determined by the time aperture of the grating and not by the duration of the ultrashort pulse (giving rise to a simplified detector response time on the order of 100 ps).

To determine the capacity of a fiber link employing a parallel-to-serial transmitter and a serial-to-parallel receiver at its two ends, several additional design issues have to be introduced. The spatial separation in the transmitter parallel channels, Δ, is found by specifying a tolerable crosstalk between channels in the receiver. The number of bit pulses in a packet depends on the numerical aperture of the optical fiber and the diameter of the optical beam, which in turn will also determine the focal length of the coupling lens to the fiber. This analysis shows that, as expected, with short duration pulses (τ small, large bandwidth) more bit pulses can be compressed into a single packet, and furthermore that we can utilize a significant portion of the optical bandwidth as information bandwidth, illustrating the efficiency of this transmission method.

Terabit Image transmission through a n optical fiber link

Transmission of a complex amplitude one dimensional (1-D) parallel data array or a 1-D image through a single-mode fiber is an important but challenging task, because the small entrance pupil of optical fiber limits coupling of signal's spatial modes. A common approach uses Wavelength Division Multiplexing (WDM), that encodes spatial information directly onto the different spectral components of a broadband point source. The idea of WDM is simple and easy to implement in a single mode optical fiber, but since it is an incoherent technique, only magnitude information of the complex amplitude spatial signal can be transmitted. In contrast, a

coherent technique would transmit both amplitude and phase of a 1-D complex amplitude signal. Lukosz introduced a technique which combines the temporal frequency bandwidth with the spatial frequency bandwidth, resulting in an optical system that permits resolution exceeding that allowed by its aperture. This approach, known as superresolution, is capable of sending complex amplitude signals over a diffraction limited aperture (e.g., a single-mode fiber) by holographic recording and reconstruction of the complex signals at the receiver. However, the requirement of reconstructing images from a hologram limits data transmission from real-time operation. In this letter, we present a novel approach that combines the advantages of both WDM and Lukosz's superresolution technique, allowing real-time parallel transmission of 1-D, complex amplitude signals through a single-mode optical fiber. Furthermore, we demonstrate experimentally that this technique is capable of transmitting, through a single-mode fiber, image depth information encoded on the input optical signals.

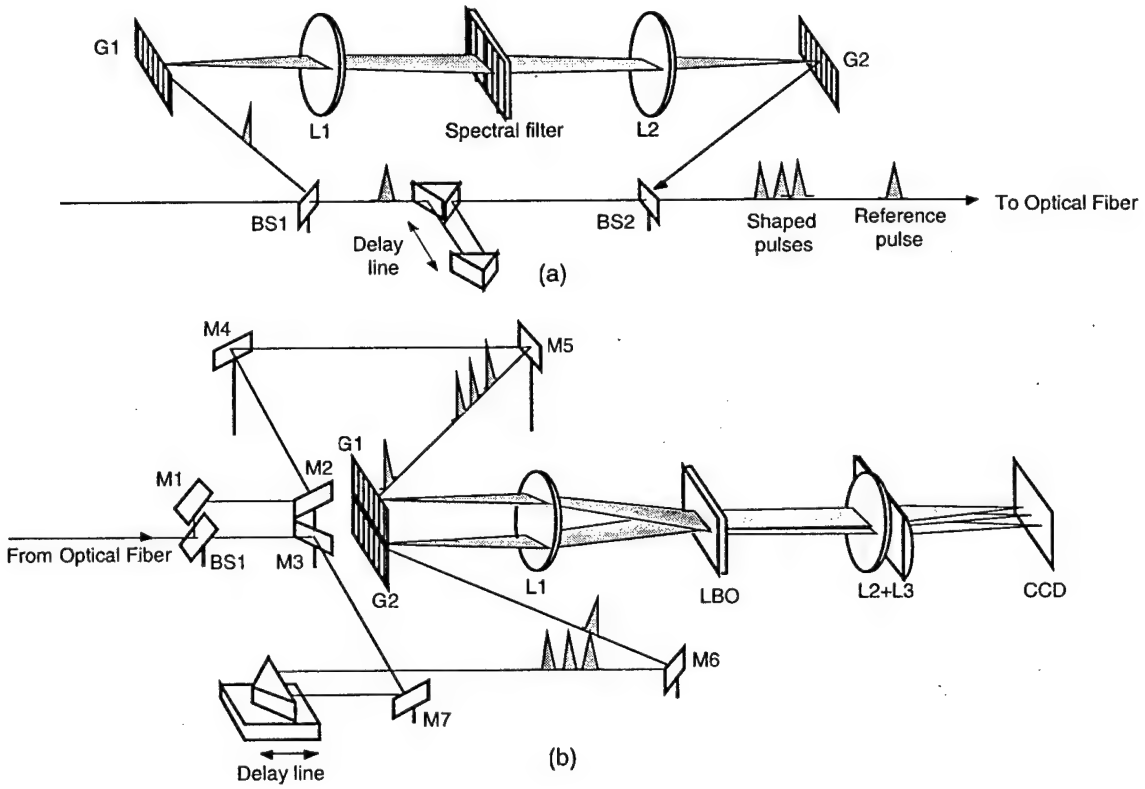

Fig. 9 Schematic diagram of optical processors for imaging through a single mode fiber: (a) a pulse shaper and (b) a pulse imager.

Our approach uses a pair of space-time conversion processors (see Fig. 9), a femtosecond pulse shaper at the transmitter and a femtosecond pulse imager at the receiver. The pulse shaper is designed in analogy with the coherent spatial Fourier optics 4-F filtering system. The pulse shaper system shown in Fig. 9a consists of a pair of spectrum decomposition devices (G1-L1 and G2-L2) in combination with a spectral domain filter. The desired pulse shape at the output is obtained by using a properly designed complex amplitude spatial filter in spectral domain to modulate the complex amplitude of the temporal frequency spectrum of an incident transform limited pulse. The spectral filter can be implemented using either a fixed or programmable mask, or can be prepared holographically similar to that of a Vander Lugt filter. Note that the Fourier spectral filter has to be updated at very high speed to achieve real-time operation. Current research on using photorefractive multiple quantum well devices for pulse shaping may

provide a solution for this requirement. The shaped pulse from the transmitter (see Fig. 9a) is sent through a single-mode optical fiber to the receiver (see Fig. 9b), where a pulse imager is employed to convert the temporal information of the shaped pulse back into the spatial domain. This conversion is based on the nonlinear optical three-wave mixing of spatially spread and inverted temporal spectrum of the shaped and the reference pulses. The nonlinear interaction generates a quasi-monochromatic second harmonic field with its spatial frequency spectrum proportional to that of the temporal frequency spectrum of the shaped pulse. A spatial Fourier transformation of the generated second harmonic field produces a spatial image that resembles the temporal structure of the shaped pulse.

In the experiment we use pulses of 200 femtoseconds at a 920 nm center wavelength , generated from a mode-locked Ti:Sapphire laser (Coherent Inc., Mira 900). The laser output is first expanded, collimated, and then split into two beams. The first beam is used as a reference beam (or clock pulse), while the second beam is used as a transform limited input pulse to the pulse shaping device shown in Fig. 9a. The shaped output pulse and the reference pulse beams are then combined collinearly in space but separated in time to avoid interference. These collinear beams are guided into a 1 meter long single-mode fiber and transmitted to the receiver.

At the receiver (see Fig. 9b), the beam exiting from the fiber is passed through a polarization compensator to restore its original polarization. The polarization-compensated fiber output is then split into two beams, both consisting of the shaped and the reference pulses. These two beams are then introduced into the pulse imager. The pulse imager setup is similar to that of discussed in Fig. 8, where a nonlinear optical LiB_3O_5 (LBO) crystal (Super Technology Inc.) is used in the Fourier transform plane of a three-wave mixing arrangement. The delay line in the second beam is used to synchronize the shaped pulse from the first beam and the reference pulse from the second beam such that they appear simultaneously on the LBO crystal, generating the output second harmonic field. In contrast, the reference pulse from the first beam and the shaped pulse from the second beam will not generate the second harmonic field, because they do not arrive onto the crystal simultaneously. The generated second harmonic field propagate in a vertical bisector direction which coincides with the optical axis of the system. A horizontal slit, a Glan-Thompson polarizer, and a narrowband color filter are used to provide three stages of filtering for separating the second harmonic signal from the fundamental frequency light of the two input beams. An inamorphic imaging of the output second harmonic field is obtained by a spherical-cylindrical lens combination (L2-L3), which performs a spatial Fourier transform in the horizontal direction and images in the vertical direction, producing an output pulse image detected by a CCD camera.

In our initial experiment on transmitting a 1-D image through a single-mode fiber, we first use as the spectral filter in the pulse shaping device a 50/50 binary amplitude grating (i.e., a Ronchi grating). Such gratings have a unique property that its Fraunhofer diffraction pattern does not have even diffraction orders except for the zeroth order. From the experimental results we obtain the intensity profile (see Fig. 10a) of the pulse image which clearly shows that the even order pulses in the sequence (besides the 0th order) do not appear. The three central pulses (i.e., -1, 0, +1 orders) are close together while the pulses corresponding to higher orders are separated by twice the distance. This experimental result demonstrates the capability of our system to perform parallel 1-D imaging through a single mode fiber.

In the second experiment we use in the pulse shaper with a spectral filter implemented by an off-axis 1-D binary phase diffractive lens. The off-axis diffractive lens was designed to produce uniform diffraction efficiencies for the -1st, the 0th, and the +1st diffractive orders, respectively corresponding to a negative quadratic phase, a constant phase, and a positive quadratic phase function. The off-axis configuration introduces a constant linear phase difference between the adjacent diffraction orders, which in turn produces a relative time delay between the three corresponding pulses at the output of the pulse shaper. The pulse shaper

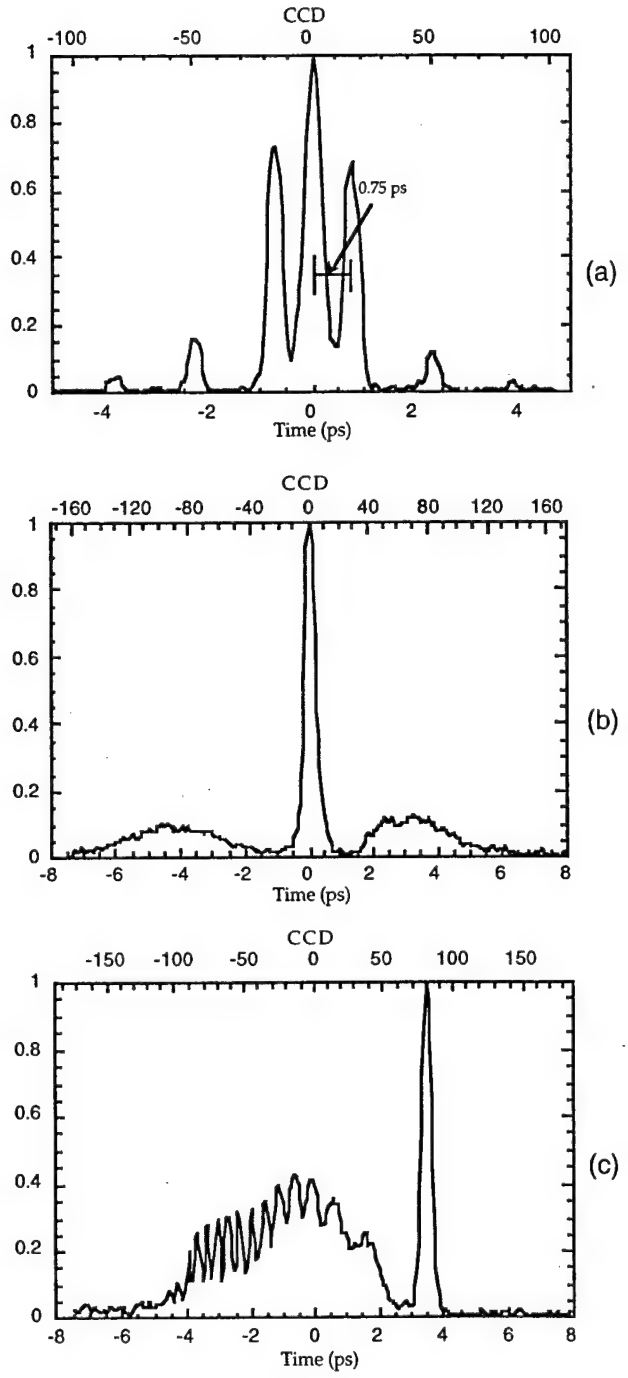

Fig. 10. Experimental results of 1-D image transmission through a single-mode fiber. (a) intensity profile of a shaped pulse image generated by a pulse shaper with a spectral filter implemented by a Ronchi grating, (b) intensity profile of a shaped pulse image generated by a pulse shaper with a spectral filter implemented by a 1-D diffractive lens, and (c) the same shaped pulse image as (b) but recorded at a longitudinally shifted observation plane where the negative chirped pulse is focused.

output consists of a sequence of three temporally separated negative chirped, transform-limited, and positive chirped pulses, again corresponding to the -1st, the 0th, and the +1st diffraction orders, respectively. Fig. 10b shows the pulse image recorded by the CCD camera located in the exact image plane of the pulse imager device (plane 1 of Fig. 9b). As expected, the detected image consist of three pulses with a transform limited pulse in the middle between the images of the positive and the negative chirped pulses. The images of the positive and negative chirped pulses are asymmetric and weaker in amplitude than the transform limited pulse due to angular dependence of the field coupling into single-mode optical fibers. By translating the CCD camera backward in the longitudinal direction to plane 2 of Fig. 9b, the image corresponding to the negative chirped pulse becomes narrower with a width corresponding to that of a transform-limited pulse, while the other two pulses become wider (see Fig. 10c). This phenomenon has been known as space-time duality which implies that the group-velocity dispersion in temporal domain is equivalent to the Fresnel diffraction in spatial domain. Figure 10c also shows that the generated second harmonic fields corresponding to the different shaped pulses can interfere with one another, indicating that the second harmonic field is quasimonochromatic and coherent.

Material dispersion can affect the performance of our technique for real-time imaging through the fiber. In principle, the introduced group dispersion can be compensated by a pulse shaper at the receiver or by using a dispersion compensation fiber. Since our technique uses transmission of both the shaped and the reference pulses through the same single-mode optical fiber, shapes of both pulses will be affected identically by the fiber material dispersion (assuming linear effects). Therefore, the shaped and the reference pulses transmitted through such a fiber can be described as

$$u_{s,r}^{(o)}(t) = \boldsymbol{F}_{\omega}\left[U_{s,r}^{(i)}(\omega)M(\omega)\right] = u_{s,r}^{(i)}(t) \otimes m(t), \tag{3}$$

where $\boldsymbol{F}_{\omega}$ denotes the temporal frequency Fourier transform operator, the superscript i and o distinguish the input and the output of the optical fiber, the subscript s and r distinguish the shaped and the reference pulses, $u_{s,r}^{(i)}(t)$ and $U_{s,r}^{(i)}(\omega)$ are the time (t) signal and the corresponding temporal frequency (ω) spectrum, while m(t) and M(ω) are the impulse response and the temporal frequency transfer function of the optical fiber, respectively. Note that in Eq. 3 we discount the carrier frequency of the short pulse, which means that the temporal frequency spectrum is centered at the carrier frequency of the short pulse. The transfer function of the optical fiber can be described by

$$M(\omega) = \exp[-jk(\omega)L] = \exp\left\{-j\left(\sum_{n}\omega^{n}k_{n}\right)L\right\}, \tag{4}$$

where $k(\omega)$is the propagation constant for each spectral component of the pulses propagating in the optical fiber, L is the length of the optical fiber, and the right hand side of Eq. 4 is obtain using Taylor series expansion of $k(\omega)$ with coefficient k_n. Next consider introducing the shaped pulse and the reference pulse from the fiber output into the pulse imaging system of Fig. 9b. The shaped pulse image is determined by the spatial Fourier transform of the second harmonic field which in turn is proportional to the product of the inverted signal and the reference spectrum amplitudes at the receiver, described by

$$\begin{aligned} u_{img}(x) &= \mathbf{F}_{\omega}\left\{U_{s}^{(i)}(-\omega)M(-\omega)U_{r}^{(i)}(\omega)M(\omega)\right\}_{t=\gamma x} \\ &= \mathbf{F}_{\omega}\left\{U_{s}(-\omega)U_{r}(\omega)\exp\left[-j2\left(k_2\omega^2 + k_4\omega^4 + k_6\omega^6 + \ldots\right)L\right]\right\}_{t=\gamma x} \\ &= \left\{\left[u_{s}^{(i)}(-\gamma x) \otimes u_{r}^{(i)}(\gamma x)\right] \otimes h(\gamma x)\right\} \otimes \exp\left[j\frac{\gamma^2 x^2}{8k_2 L}\right], \end{aligned} \tag{5}$$

where γ accounts for the time-to-space conversion (i.e., $t=\gamma x$), and $\otimes$ denotes the convolution operator, and we also neglect constant phase and $h(\gamma x)$ represents the impulse response function of all dispersion components larger than $n \geq 4$ order. We observed from Eq. 5 that only the even order terms of the Taylor expansion of propagation constant can affect the result of the pulse imaging system, whereas all the odd order terms are canceled out. The result of Eq. 5 also indicates that the second order effect of the group velocity dispersion from the optical fiber can be eliminated by a longitudinal translation of the image observation plane by a distance $z = \frac{8\pi k_2 L}{\lambda_c \gamma^2}$, where λ_c is the center wavelength of the pulse beam. In the new observation plane the image of the shaped pulse transmitted through the dispersive fiber will be identical to that obtained without group dispersion, assuming negligible higher order dispersion coefficients (i.e., $h(\gamma x) = \delta(x)$). Furthermore, when the effect of high order dispersions can not be neglected, they can be easily compensated in space domain by properly designed fixed or programmable phase masks, because the time domain dispersion effects have been transferred into space domain, acting as spatial aberrations.

We have introduced and experimentally demonstrated a novel imaging technique that allows us to transmit a 1-D image through a single-mode optical fiber. In contrast to the WDM technique, our approach preserves both amplitude and phase information of optical signal transmitted through the fiber. This unique property enables encoding of the input signal in the longitudinal direction (i.e. depth) in addition to the commonly used transverse direction. The effect of the fiber material dispersion on our imaging technique is analyzed and potential solutions are discussed.

Nonvolatile spectral holography for time domain storage of femtosecond pulses.

Many applications will benefit from an optical holographic memory that will store and retrieve information in a format that is suitable for direct interface and transmission through an optical fiber network, thereby, providing optimal performance in terms of hardware complexity, memory and network capacity, bandwidth, and latency. With such approach the spatial image information is converted to time domain sequence and stored as a spectral hologram. The information retrieved from the memory, occurs at the output in a time sequence format, suitable for direct transmission over an optical fiber network at rates exceeding 1 Tbits/sec. At the network receiver node, the time sequence data can be demultiplexed by converting the time sequence back to parallel spatial channels for electronic detection, processing and display.

Fig. 11 shows the experimental setup for storage of femtosecond pulses using spectral holographic recording in a 1 mm thick iron-doped photorefractive lithium niobate crystal. Recording is performed using 460 nm wavelength of a frequency doubled Ti:Sapphire laser pulses of 200 fsec at a center wavelength of 920 nm. The second harmonic beam is divided into a reference and a signal beams. The signal beam is transmitted through a pulse shaping device that introduces the temporal information sequence. Both beams are then directed into the system of Fig. 11 for spectral holographic recording. We use an exposure time of 2 minutes, yielding a diffraction efficiency of about 7%. The hologram is readout using 200 fsec laser pulses at a center wavelength of 920 nm to avoid erasure during the readout. The incidence angle of the readout beam is adjusted to satisfy the Bragg matching conditions of the recorded spectral hologram. The readout time domain information is then measured employing an ultrashort pulse optical cross correlation, where one of the beams is a fraction of a transform limited readout beam, while the other beam is the resultant memory readout signal.

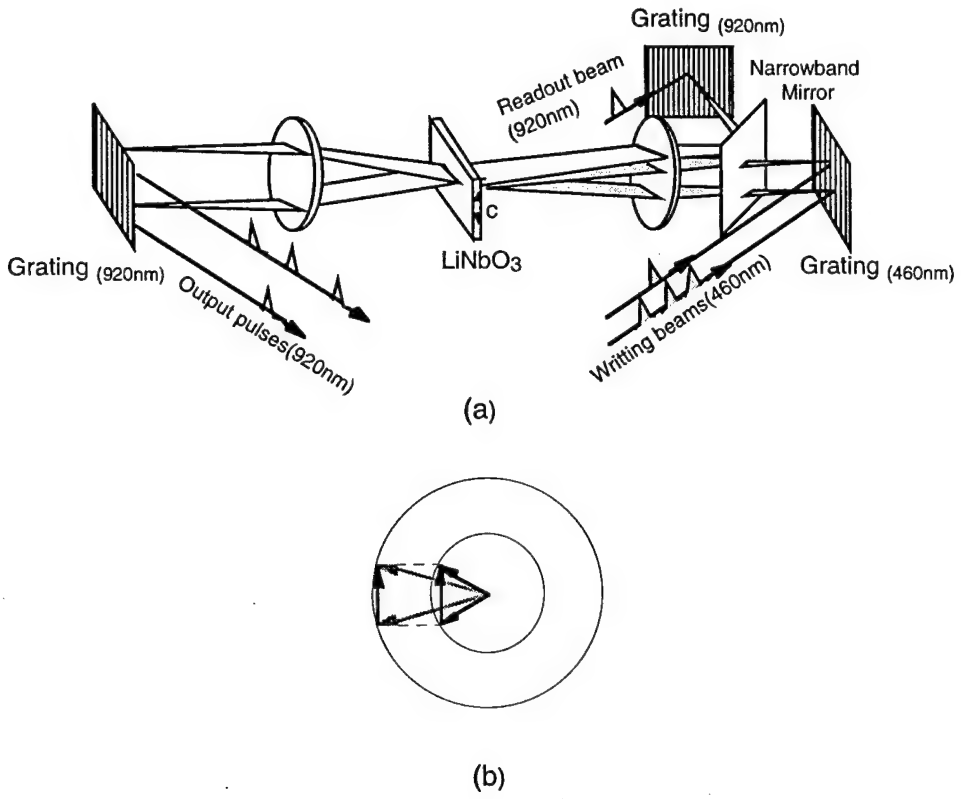

Fig. 11. Schematic diagram of the experimental setup: (a) spectral hologram of a sequence of femtosecond pulses is recorded in a 1 mm thick photorefractive crystal of lithium niobate using frequency doubled 200 fsec pulses at center wavelength of 460 nm. Nonvolatile reconstruction is obtained with 200 fsec pulses with center wavelength of 920 nm; (b) k-space describing the recording and reconstruction geometries.

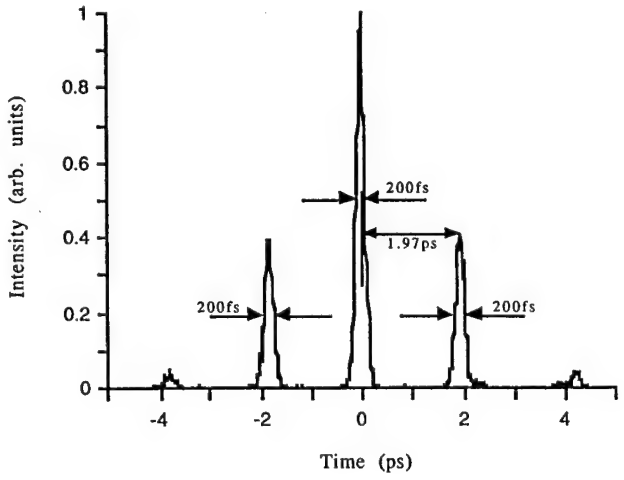

Fig. 12. The crosscorrelation traces of pulse sequence reconstructed from the spectral domain hologram when the recorded sequence was obtained from a pulse shaper with Ronchi grating.

In our first experiment we store a sequence of pulses obtained from using a Ronchi grating in a pulse shaper. Figure 12a shows the crosscorrelation of the pulse sequence reconstructed from the spectral domain hologram, demonstrating good performance. Each pulse has transform limited width of 200 fsec. The recorded spectral domain holograms were readout for over 24 hours without degradation, indicating that the photorefractive hologram recorded with 460 nm wavelength is insensitive to the readout wavelength of 920 nm.

In summary, we have introduced and experimentally demonstrated a 4-wave mixing optical processor that performs both parallel-to-serial and serial-to-parallel data conversion. To meet the speed requirements using existing nonlinear optical materials, we also constructed a nonlinear 3-wave mixing optical processor that performs imaging of 1-D femtosecond optical pulses with femtosecond time response. We conducted experiments on transmission of the time multiplexed signal sequences through fiber. This signals have been used in our 3-wave mixing demultiplexer and converted to parallel spatial channels for electronic detection. Our method of multiplexing and demultiplexing relies on transmission of a reference pulse, which in turn introduces two very important advantages relevant to third-generation optical network systems: (i) the linear dispersion due to transmission through fiber is compensated during the detection process and (ii) the reference signal serves as synchronization signal resolving issues of network synchronization.

In the future we are planning to continue our investigation of spectral domain nonlinear optical processing using three- and four wave mixing. The ongoing work is also focusing on analyzing the spectral domain optical processors in terms of their performance characteristics such as resolution, time-bandwidth product, speed, parallelism, dispersion, efficiency, etc. We also are planning to investigate effect of optical amplifiers on transmission of ultrashort optical pulses. Finally, we also plan to explore fast optical nonlinearities of semiconductors and semiconductor nanostructures for spectral domain mixing of femtosecond pulses.

C. Network Security and Privacy

The work at UCSD on network security and privacy was focused primarily on quantum cryptography for secret key generation and exploration of chaotic systems for implementing privacy.

Quantum cryptography for secret key generation.

Quantum cryptography is a recently developed technique which permits two parties, who share no secret information initially, to communicate over an open channel and establish between themselves a shared secret sequence of bits. Quantum cryptography is provably secure against an eavesdropping attack, in that, as a matter of fundamental principle, the secret data cannot be compromised unknowingly to the legitimate users of the channel. Any attempt by a third party to monitor a quantum cryptographic channel reveals itself through transmission errors between the legitimate users.

A realistic communication is not completely free of losses and errors even if no eavesdropping is present. Nevertheless, it is possible to conduct a provably, unconditionally secure quantum cryptographic conversation over a realistic channel of reasonable quality, albeit at a reduced throughput. This is accomplished with the aid of a three-step operational scheme, which we shall refer to as *key distillation*. This scheme involves negotiation between the legitimate users, referred to as Alice and Bob, over a separate, open channel. Having (openly) discarded those bits of the transmission for which Bob's measurement yielded an inconclusive, and therefore useless, outcome (such bits are an inevitable byproduct of a quantum cryptotransmission), Alice and Bob begin the first, *error correction* step of the scheme (Fig. 13). Error correction is accomplished through an open exchange of messages, such as a series of checksums, which permit Alice and Bob to locate and remove errors from the raw quantum transmission without revealing the data in its entirety. Next, based on the observed error rate, and based on their assumptions about possible eavesdropping strategies, Alice and Bob make a worst case estimate of the amount of information on the corrected data that an eavesdropper (known as Eve) may possess. This estimate is used in the third and final step, where Alice and Bob employ a protocol known as *privacy amplification* to compress the data in such a way that Eve's knowledge of it is diminished. The amount s of data that must be sacrificed in compression depends on the desired level of security and on Alice and Bob's worst case estimate of Eve's knowledge (more precisely, Renyi information) on the corrected data prior to compression.

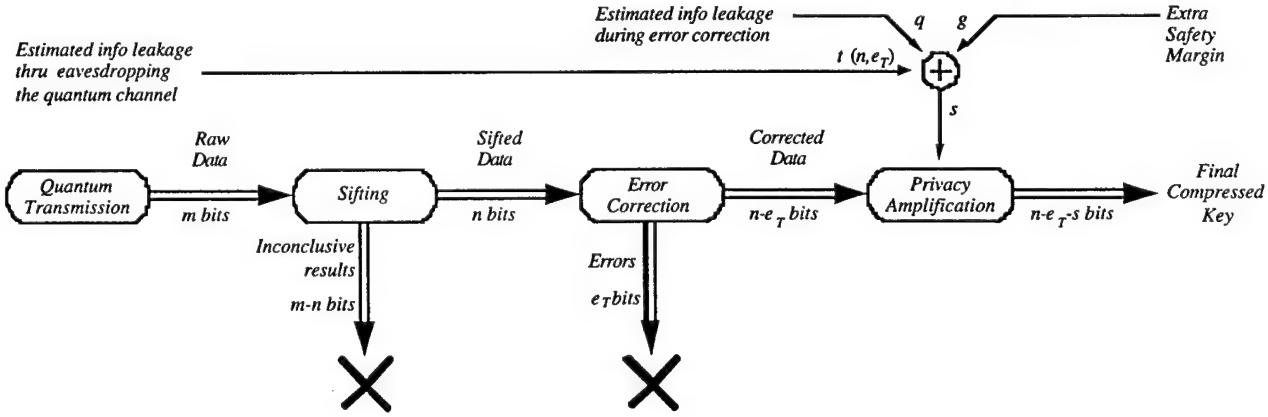

Fig. 13. Distillation of secret key from a quantum transmission. Alice and Bob arrive at privacy amplification compression level s by summing estimates of possible information leakage at various stages of the protocol, together with an arbitrary safety margin.

The ultimate figure of merit of a cryptographic key exchange process is its *secrecy capacity*, which can be defined as the number of shared secret bits produced per unit time, or alternatively, per bit transmitted through the physical channel. Secrecy capacity of a quantum cryptosystem is affected by a host of factors (some of them illustrated in Fig. 13), including adopted estimates of information in Eve's possession, error correction algorithm employed, as well as line attenuation, detector quality, and the expected fraction of inconclusive outcomes. We obtained a general expression for secrecy capacity accounting for these effects based on the best available approximations of information leakage and error correction costs. Secrecy capacity was found to strongly depend on channel error rate and detector efficiency; specifically, it was found that performance degrades dramatically at error rates above 5%.

More accurate assessment of information leakage and error correction costs leads to a better estimate of secrecy capacity. Leakage estimates are also important in their own right, because Alice and Bob must use them during key distillation as explained previously. These estimates, and related issues, are the subject of our current work.

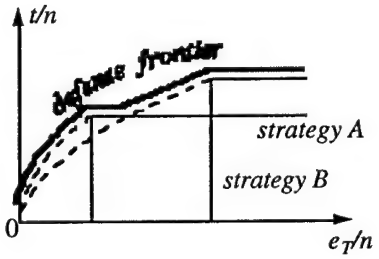

Fig. 14. Defense Frontier $t(n,e_T)$.

One set of problems under investigation is that posed by information leakage through possible eavesdropping on the quantum channel. We have developed for the first time the rigorous definitions and the mathematical formalism for making such estimates. According to our scheme, Alice and Bob analyze each of the anticipated eavesdropping strategies for its intrusiveness (the error rate likely to result from it), and its yield (the amount of information an eavesdropper is likely to gain). Such an analysis, which is based on the joint probability distribution of Bob's and Eve's outcomes, requires a quantum mechanical definition of the strategy. This description however, can remain quite generic. The task is easily accomplished, for example, with respect to any strategy yet described in the literature. We demonstrate how intrusiveness and yield measures lead to a *defense function* for a given strategy. Alice and Bob's adopted estimate of information leakage through eavesdropping $t(n,e_T)$, which we call the *defense frontier*, is a function of their observed error rate such that it lies above and to the left of the defense functions constructed for all anticipated eavesdropping strategies (Fig. 14). As shown in Fig.13, the defense frontier must be taken into consideration by Alice and Bob when deciding the amount of compression necessary to protect their key, which in turn affects secrecy capacity of the system.

Data loss at the privacy amplification stage, and with it the secrecy capacity of the system, are also affected by Alice and Bob's adopted estimate of the amount of information possibly leaked during error correction. If error correction is accomplished through an open exchange of a series of checksums, Alice and Bob can crudely upper bound the leakage during a given communication by the number of checksum bits publicly exchanged. For (*a priori* average) secrecy capacity estimation, however, not the actual but the statistically expected number of checksum bits is required. This expected value depends not only on the number of errors to be corrected, but also on the details of the correction protocol, and on the desired level

of confidence in the result. Both the formalism of such an analysis and its application to specific protocols are currently under investigation.

Our experimental work concentrated on a frequency division multiplexed (FDM) long distance interferometry (LDI) implementation of quantum cryptography. The FDM scheme is suitable for use in an optical fiber, because information is encoded on the phase difference between the signals at two closely spaced optical frequencies, which is expected to transmit reliably through a fiber without being significantly affected by environmental factors. We have investigated this assumption experimentally by subjecting a fiber to controlled temperature stress in the laboratory. We also assembled a prototype FDM LDI on an optical table from standard components, including photomultiplier tubes for single photon detection. Future plans include a wavelength division multiplexed multichannel quantum cryptographic realization utilizing polarization.

Security of quantum cryptography in a noisy environment

We investigated the relationship between the induced error rate and the maximum amount of information the eavesdropper can extract, both in the two-state B92 and the four-state BB84 quantum cryptographic protocols. Analysis was limited to eavesdropping strategies where each bit of the quantum transmission is attacked individually and independently from other bits. Subject to this restriction, however, we believe that all attacks not forbidden by physical laws are taken into account. For both B92 and BB84, we explicitly constructed the optimal eavesdropping method that on average yields the most information for a given error rate. In each case, a closed-form functional dependence between the error rate and the information yield was found, and confirmed by numerical simulation. This result is illustrated by solid lines in Figs. 15 and 16, where it is compared with information yields on bits not in error for some other previously published eavesdropping strategies. The relationship between the induced error rate and the eavesdropper's information on error-free bits can serve as input for the construction of the defense frontier, which has been suggested in our earlier work as a formalism for securing a quantum cryptographic transmission in a noisy environment.

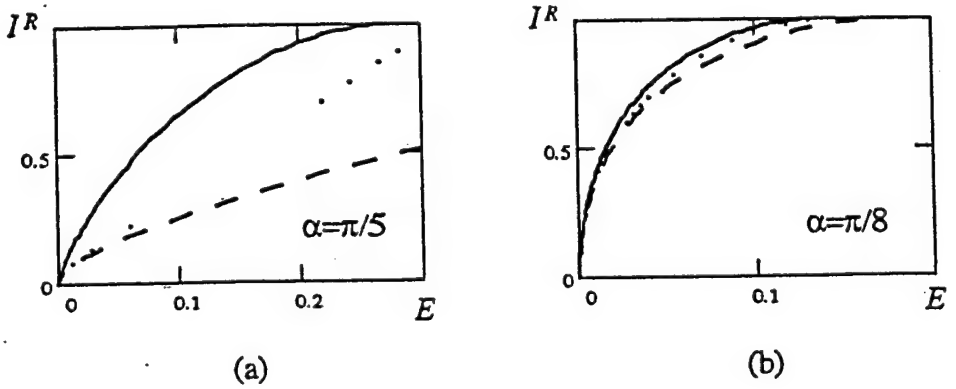

Fig. 15. Eavesdropper's information I^R on error-free bits versus the error rate E in B92: the UCSD result (solid); "translucent eavesdropping with entanglement" due to Peres (dotted); the FP96 attack due to Peres (dashed).

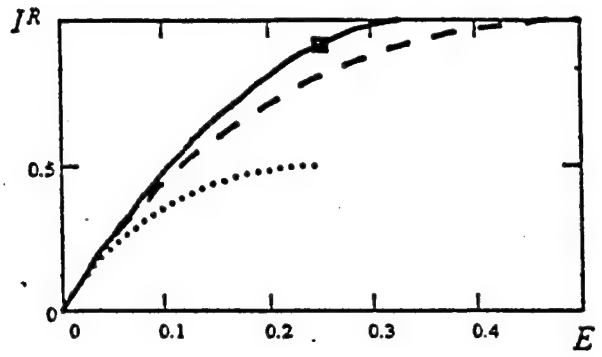

Fig. 16. Eavesdropper's information I^R on error-free bits versus the error rate E in BB84: the UCSD result (solid); Breidbart basis attack (box); "measurement of intensity g" due to Huttner (dotted); the FGGNP97 attack due to Fuchs (dashed).

Evaluation of the cost of error-correction protocol in quantum cryptographic transmission

After the initial raw quantum cryptographic transmission, the legitimate users Alice and Bob are in possession of a string of bits which can then be further refine to extract the key. The process of refinement comprises as a first stage correction of all the errors: indeed errors are very likely because of the single photon transmission and because of the possible presence of the eavesdropper Eve whose eavesdropping activity is visible through increasing the number of errors. We concentrate here on analyzing the bisect-and-discard error-correction protocol relying on disclosing the parity of blocks of bits and discarding bits so that the errors are corrected.

Assume that the quantum crypto-transmission has yielded a string of N raw bits shared between Alice and Bob. Assume further that some of the bits were publicly disclosed in order to estimate the error rate and the error rate was found to be $r=N/K$ meaning that it was estimated that there were K errors among those N bits. The task is using the bisection and parity disclosure procedure proposed to remove the K errors. The string of bits is first divided into blocks of p bits whose parity is checked: in case of parity mismatch the block is divided into two halves and the parity is again checked-this bisection and parity check proceeds until the block are only two bits long. In case of a parity match, one bit is discarded and the parity of the next block is examined.

We derive the analytic expression for the bound on the probability that j-bit are in error. The crucial hypothesis in the derivation of the analytical expression was that we can calculate the average in the next iteration using the average of the previous one. To test this hypothesis, we have written a Monte Carlo simulation of the error correction procedure. Given the number of raw bits N and the estimated number of errors K, we first generate K random numbers uniformly distributed over the string of bits. The block size is chosen to be $p=N/K$ and the parity check and discarding of bits is simulated for every block of the string. At the end both, the number of corrected errors and the number of discarded bits are computed and the new values of N and K are calculated. The simulation then generates new random numbers representing the errors and bisection is again commenced until all the errors have been removed.

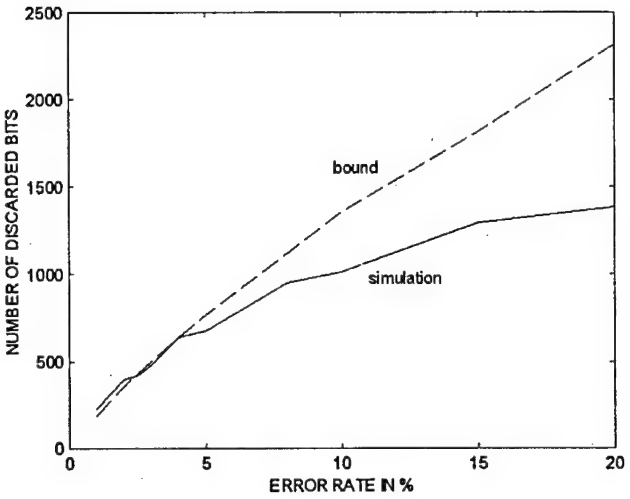

Figure 17. The cost of performing the error correction (in number of discarded bits) as a function of the error rate, 2000 raw bits were transmitted: full line - simulation; dashed line - the analytical expression.

Figure 17 gives a comparison between the simulations and the analytical expression curve in terms of the cost of performing the error correction (represented by the number of discarded bits necessary to remove the errors) versus the error rate. For fair comparison and in order to obtain average quantities, the simulation was run for 1000 transmissions and the average number of discarded bits was computed. The results are represented with full line for the simulation results and dashed line for the analytical expression. The agreement between the two results is very good for small error rates. For large error rates the analytic prediction gives increasingly poor results due to inaccuracy of the approximation $p_i = 2p_{i-1}$. Note that above 15% error rate out prediction indicates that all the bits should be sacrificed for performing the error correction (originally 2000 raw bits were established). Other protocols, most notably using pre-determined block sizes based on estimate of the error rate in every iteration are being implemented.

Chaotic systems for privacy of optical networks

Report on chaos for secure communications In this project, we study the use of chaos in semiconductor laser for secure communications. In particular, we investigate ways to generate controlled chaos in laser diodes for use in synchronized chaos schemes. We have previously found that deliberately detuned lasers or laser system can generate chaotic or quasi-chaotic instability, which can hide transmitted signals to secure optical communication. In prior work, we used Lang-Kobayashi equation to analyze chaotic instability in external cavity mode-locked lasers. Even though it predicts generation of chaos under certain modulation conditions, the route to chaos is somewhat different from what we observed experimentally. Therefore we re-examine the model more closely in this work. The Lang-Kobayashi type of analysis largely has ignored spatial dependence of the electromagnetic fields in laser cavity and so it is inadequate to describe very high speed switching or transient behaviors that lead to chaos. The subtle relation between the nonlinear gain and the electromagnetic field is usually overlooked in the Lang-Kobayashi type of analysis. In this program, we have developed and implemented a new classical method, Green's function method, which is capable of trucking time history of the position dependent electromagnetic fields generated inside active dielectric media with multiple boundaries at any frequencies. With this method, we will be able to accurately model wide variety of chaotic or quasi-chaotic instability inside or outside laser resonators and examine interactions between multiple lasers (e.g. synchronization) by extending the one-laser systems into two-laser or multiple-laser configurations.

5. Personnel Supported

Y. Fainman, PI, Professor

A. Kellner, co-PI, Assistant Research Scientist

L. Milstein, Director - Graphics Server Consortia, Professor

W. S. C. Chang, Research Professor

R. Cruz, Associate Professor

R. Rao, Associate Professor

P. K. L. Yu, Professor

P. Cosman, Assistant Professor

P. Seigal, Professor

P. C. Sun, Assistant Project Scientist

Y. T. Mazurenko, Visiting Research Physicist

T. Suzuki, Postgraduate Research Engineer

L. Tancevski, Postgraduate Research Engineer

F. Xu, Postgraduate Research Engineer

B. Slutsky, Research Assistant

A. Merriam, Research Assistant

D. Schilling, Research Assistant

D. Marom, Research Assistant

G. Kuan, Research Assistant

P. Lin, Research Assistant

H. Rao, Research Assistant

P. Shames, Research Assistant

R. Tyan, Research Assistant

Q. Hyang, Undergraduate Research Assistant

J. C. Johnson, Undergraduate Research Assistant

6. Publications

P. C. Sun, Y. Mazurenko and Y. Fainman "Long-distance frequency-division interferometer for communication and quantum cryptography," Opt. Lett., **20**, 1062-1964, 1995.

P. C. Sun, Y. Mazurenko and Y. Fainman "Transmission of optical phase information using frequency division of signals with application to quantum cryptography," Sov. Optics and Spectroscopy, v. **78**, #6, 1995.

P. C. Sun, Y. Mazurenko, W. Chang, P. Yu and Y. Fainman "All-optical parallel-to-serial conversion by holographic spatial-to-temporal frequency encoding," Opt. Lett., 20, 1728-1730, 1995.

S.M. Perlmutter, P.C. Cosman, R.M. Gray, et al., "Image quality in lossy compressed digital mammograms," Signal Processing, Special issue on medical image compression, submitted 1996.

J. Strom and P.C. Cosman, "Medical Image Compression with Lossless Regions of Interest," Signal Processing, Special issue on medical image compression, to appear 1996.

L. Tancevski, A. L. Kellner, R. Rao, Y. Fainman and R. L. Cruz, "Reduction of Four-Wave Mixing Noise in WDM Optical Networks," submitted to IEEE J. Lightwave Technology, 1996.

B. Slutsky, P.C.Sun, Y.Mazurenko, R.Rao, and Y.Fainman, "Effect of channel imperfection on the secrecy capacity of a quantum cryptographic system," J. of Modern Optics, 44, No. 5, 953-961, 1997.

P. C. Sun, Y. Mazurenko, Y. Fainman, "Femtosecond pulse imaging: ultrafast optical oscilloscope," JOSA A, 14, 1159-1169, 1997.

R. Tyan, A. Salvekar, H. Chou, C. Cheng and A. Scherer, F. Xu, P. C. Sun and Y. Fainman, "Design, Fabrication and Characterization of Form-Birefringent Multilayer Polarizing Beam Splitter" JOSA A, 14, No 7, 1627-1636, 1997.

P. C. Sun, Y. Mazurenko, Y. Fainman,"Real-time 1-D Coherent Imaging Through Single-mode Fibers by Space-Time Conversion Processors," accepted by Optics Letters, 1997.

Y. Fainman, Y. Mazurenko, and P. C. Sun, "Space-Time Optical Processing with Ultrafast Pulses," Proc. of Euro-Americal Workshop on Optical Pattern Recognition, 1997; also presented in the Euro-American Workshop on Optical Pattern Recognition, Barselona, Spain, 1-5 June, 1997 (Invited).

T. Suzuki and P. K. L. Yu, "Suppression and enhancement of elastodynamic radiation from a point source load in elastic wave band structures," J. Appl. Phys., 80(10) 15 November, 1996, p 5665- 5673.

T Suzuki and P. K. L. Yu, "Complex Elastic Wave Band Structures in Three Dimensional Periodic Elastic Media", accepted for publication in Journal of Mechanics and Physics of solids (1997).

S.M. Perlmutter, P.C. Cosman, R.M. Gray, et al, ``Image quality in lossy compressed digital mammograms," accepted for publication in Signal Processing, Special issue on medical image compression, 1997

J. Strom and P.C. Cosman, ``Medical image compression with lossless regions of interest," accepted for publication in Signal Processing, Special issue on medical image compression, 1997.

T. Suzuki and P. K. L. Yu,"Method of Projection Operators for Photonic Band Structures with Perfectly Conducting Elements", submitted to Physical Review B (1997).

D. Marom, P. C. Sun, Y. Fainman, "Analysis of spatio/temporal converters for all-optical communication links," submitted to Appl. Opt.

B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and Y. Fainman, *Defense Frontier Analysis of Quantum Cryptographic Systems*, Appl. Opt. (submitted).

B. Slutsky, R. Rao, P.-C. Sun, Y. Fainman, *Security of quantum cryptography against individual attacks*, Phys. Rev. A (submitted).

7. Interactions/transitions

a. Meetings, Conferences, Seminars, Proceedings

P. C. Sun, Y. Mazurenko, and Y. Fainman, "All optical parallel-to-serial conversion by holographic spatial-to temporal requency encoding," OSA 1995 Topical Meeting on Optical Computing, Salt Lake City, Technical Digest, 1995.

Y. Fainman, P.C. Sun, Y. Mazurenko, D. Brady, "Space-time processing with photorefractive volume holography," presented at the SPIE's 40-th Annual Meeting, San Diego, July 1995; Proc. SPIE, conf. 2529, 1995 (invited).

B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainman, " Long-distance frequency-division interferometer for communication and quantum cryptography," presented at the OSA Annual Meeting, Portland, September 1995.

P. C. Sun and Y. Fainman, "Properties of holographic space-time signal processing," presented at the OSA Annual Meeting, Portland, September 1995.

A. L. Kellner, R. L. Cruz, Y. Fainman, R. D. Fellman, Y. Muzurenko, L. B. Milstein, R. R. Rao, P. C. Sun, and P. K. L. Yu, "Transparent terabit photonic imaging networks," Proc. SPIE, 2690, 118–124, 1996.

B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainman, "Quantum cryptography for secret key generation using frequency-division long distance interferometry," presented at SPIE West'96, San Jose, 1996; also Proc. SPIE, 1996.

B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainman, "Quantum cryptography using frequency-division transmission of optical phase," CLEO/Europe'96, 1996.

D. Marom, P. C. Sun, Y. Fainman, "Temporal phase conjugation with space-time processors, " Holography," Vol.4, 1996 OSA Technical Digest Seriers, pp. 62-65, (OSA, Washington DC, 1996).

P. C. Sun, Y. Mazurenko, Y. Fainman, "Space-time processing of femtosecond optical pulses for imaging through fiber," OSA Annual Meeting 1996, Rochester, New York.

B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainman, "Quantum Cryptography in the Presence of Noise and Losses," OSA Annual Meeting 1996, Rochester, New York.

B. Slutsky, R. Rao, L. Tancevski, P. C. Sun, and Y. Fainman, "Defense Against Bitwise Eavesdropping Strategies in Quantum Cryptography," OSA Annual Meeting 1996, Rochester, New York.

B. Slutsky and Y. Fainman, "Quantum cryptography uses photons to establish secret key," intervew article in OE Reports of SPIE, News and Commentary for the International Optical Engineering Community, No. 147/March 1996.

Y. Fainman, " Space-time processing with ultra-short laser pulses for holographic storage," International Symposeum on Holographic Storage, Greece, May 1996 (invited paper).

P. C. Sun, Y. Mazurenko, Y. Fainman, "Femtosecond pulse imaging by nonlinear three-wave mixing," submitted to IEEE/LEOS Annual Meeting, 1996

P. C. Sun, Y. T. Mazurenko, and Y. Fainman,"Real-time space/time processing with femtosecond laser pulses," presented at the SPIE's Annual Meeting, Denver, paper 2849-40, August 1996; Proc. SPIE, 1996 (invited paper)

B.C. Lam, A.L. Kellner, P.K.L. Yu, M.M. Sushchik, and H.D.I. Abarbanel, "Chaotic Instabilities in Modulated External Cavity Semiconductor Lasers," SPIE Conference Proceedings, Vol. 2610, p. 13-22 (1995).

R. L. Cruz and C. Okino, "Service Guarantees for Window Flow Control," to appear in Proceedings of the 34th Annual Allerton Conference on Communication, Control, and Computing, Monticello, Il., Oct. 2–4, 1996.

A. L. Kellner, R. L. Cruz, Y. Fainman, R. D. Fellman, Y. Muzurenko, L. B. Milstein, R. R. Rao, P. C. Sun, and P. K. L. Yu, "Transparent terabit photonic imaging networks," Proc. SPIE, 2690, 118-124 (1996).

B. Slutsky, R. Rao, L. Tancevski, P. C. Sun, and Y. Fainman, " Information leakage estimates in quantum cryptography," presented at the *OSA Topical Meeting on Optics in Computing*, Incline Village, Lake Tahoe, Nevada, *Technical Digest*, p. 115-117, March 1997.

R. C. Tyan, P. C. Sun, F. Xu, A. Salvekar, H. Chou, C. C. Cheng, A. Scherer and Y. Fainman, " Subwavelength multilayer binary grating design for implementing photonic crystals," presented at the *OSA Topical Meeting on Quantum Optoelectronics,* Incline Village, Lake Tahoe, Nevada, *Technical Digest*, p. 35-37, March 1997.

Y. Fainman, Y. Mazurenko, and P. C. Sun, "Ultra-fast Space-Time Processing," presented at the *OSA Topical Meeting on Optics in Computing*, Incline Village, Lake Tahoe, Nevada, *Technical Digest*, p. 175-177, March 1997 (invited).

D. Marom, P. Shames, F. Xu, R. Rao, and Y. Fainman, ":Compact free-space multistage interconnection network demonstration," presented at the *OSA Topical Meeting on Optics in Computing*, Incline Village, Lake Tahoe, Nevada, *Technical Digest*, p. 192-194, March 1997.

K. Oba, P. C. Sun, Y. Fainman, "Nonvolatile photorefractive spectral holography for time-domain storage of femtosecond pulses," CLEO'97, v. 11, 213-214, Baltimore, 1997.

B. Slutsky, R. Rao, Y. Fainman, " Security theorems in quantum cryptography," submitted to Proc. SPIE on Computer and Network Security Conference, Dallas, Texas, November 1997.

L. Tancevski, B. Slutsky, R. Rao, Y. Fainman, " Evaluation of the cost of error correction protocol in quantum cryptographic transmission," submitted to Proc. SPIE on Computer and Network Security Conference, Dallas, Texas, November 1997.

D. Marom, P. C. Sun, Y. Fainman, "Communication with ultrashort pulses and parallel-to-serial and serial-to-parallel converters," Proc. IEEE/LEOS, to be presented at the 10-th Annual Meeting of IEEE/LEOS, 1997..

Y. Fainman, "Optical interconnect systems for communications and computing," Proc. IEEE/LEOS, to be presented at the 10-th Annual Meeting of IEEE/LEOS, 1997 (invited).

A. L. Kellner and T. R. Nelson, "Quality-of-Service Requirements for Medical Imaging Networks," SPIE - Conference on Biomedical Sensing, Imaging, and Tracking Technologies II, San Jose CA, (1997).

A. L. Kellner and T. R. Nelson, "Quality-of-Service Requirements for Diagnostic Medical Imaging," paper ThUU2, Optical Society of America Annual Meeting, Long Beach CA, (1997).

T. R. Nelson and A. L. Kellner, "High-Performance Clinical Patient Data Review and Consultation System," Medicine Meets Virtual Realty 5, San Diego CA, (1997).

R. L. Cruz and C. M. Okino, "Service Guarantees for Joint Scheduling and Flow Control," to appear in Proceedings of 36th IEEE Conference on Decision and Control, San Diego, CA, December, 1997.

A.L. Merriam, A.L. Kellner, and P.C. Cosman, ``Lossless image compression over lossy packet networks," International Conference on Signal Processing Applications and Technology (ICSPAT '97), to appear 1997

b. Consultative and advisory functions

Y. Fainman, "Optical Interconnections using broadband sources," *The First Workshop on Mutli-wavelength Free-Space Optoelectronic Interconnects,* Taos, NM, February 1996.

A. L. Kellner, "Broadband Photonic Networks for Medical Imaging," presented at BMDO Technology Applications Review: Medical, San Diego CA, 16–17 January 1996.

Y. Fainman , "Optical systems, devices and components for Security," Report for the NSF, DARPA and AFOSR workshop " The role of optical systems and devices for security and anticounterfeiting," Washington D. C., February 1996

Y. Fainman, "Space-Time optical signal processing", Optical Computing/Department of Electrical Engineering, California Institute of Technology, April 1997.

Y. Fainman "Optoelectronic systems for space variant signal and image processing," presented at the DARPA Workshop on FSOI, Arlington, May 1997.

R. L. Cruz, "SCED+: Efficient Management of Quality of Service Guarantees," Technical Report 9713, Center for Wireless Communications, UCSD, July, 1997.

R. L. Cruz, "Quality of Service Management in Integrated Services Networks," Proceedings of 1st Semiannual Research Review, Center for Wireless Communications, UCSD, June 6, 1996.

Y. Fainman "Space-Time processing using Femtosecond laser pulses," presented at Thomson CSF, Paris, August, 1997.

Y. Fainman, "Computer-Generated Holograms with Multifunctionality in Polarization and Color," Department of Electrical Engineering, Purdue University, October 1996.

8. New discoveries:

None

9. Honors/Awards:

None